ExtremeSwitching

Configuring Security on Ethernet Routing Switch 3600 Series

Release 6.4
9036476-00 Rev AA
February 2020

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 administer and configure security features for Extreme Networks ERS 3600 Series, including MAC-based security, RADIUS, EAPOL, and SSH.

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`.
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.

Table continues…

Convention	Description
	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

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware/software compatibility matrices for Campus and Edge products
Supported transceivers and cables for Data Center products
Other resources, like white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, 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: (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, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions 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

Subscribe 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 (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. Select **Submit**.

Providing Feedback

The Information Development team at Extreme Networks has 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 we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information in the document.

- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

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

There are no new feature changes in this document.

Chapter 3: Security fundamentals

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

Management password configuration

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

Console TELNET Password Configuration

With Telnet access, you can communicate with the switch as if the console terminal were directly connected to the switch. You can establish up to four active Telnet sessions at one time, in addition to one active Console connection for a total of five possible concurrent users.

Logging on

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

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

Figure 1: Setting the user name and password using CLI

Campus security example

The following figure shows a typical campus configuration using the RADIUS-based and MACaddress- based security features.

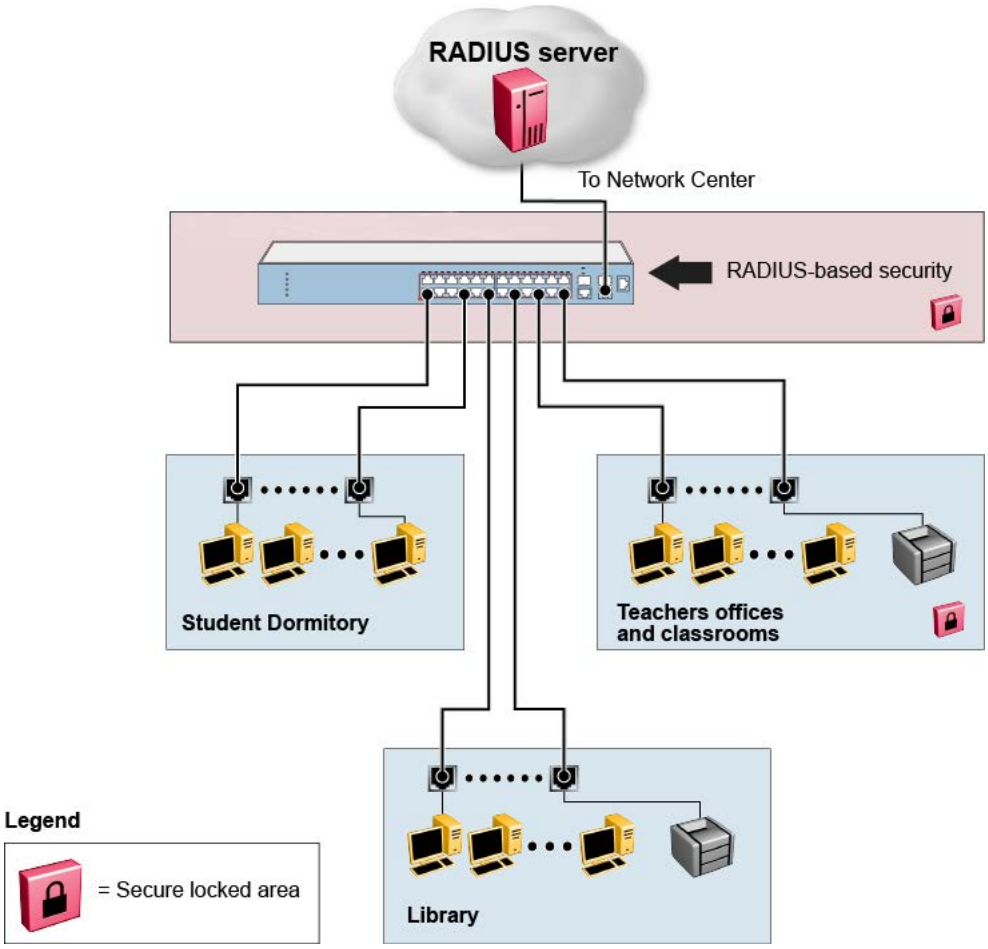

Figure 2: Security features

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

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

- The switch
  - RADIUS-based security is used to limit administrative access to the switch through user authentication (see RADIUS-based network security on page 164).
  - MAC address-based security is used to allow up to 448 authorized stations (MAC addresses) access to one or more switch ports (see MAC address-based security on page 78).
  - The switch is in a locked closet, accessible only by authorized Technical Services personnel.
- Student dormitory

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

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

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

Password security

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

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

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

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

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

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

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

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

Custom user names and passwords

Custom user names and passwords can be created for accessing the switch or stack. User names and associated passwords can be defined at any time but only come into effect when password security is enabled. User names and passwords are created only by a user with read-write privileges.

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

Log on failure timeout

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

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

Password security

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

When you enable password security, the following happens:

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

When you disable password security, the following happens:

- Current passwords remain valid.
- Password verification is not required.

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

Password length and valid characters

Valid passwords are from 10 to 15 characters long. The password is 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.

Password aging time

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

Password check sequential and repeated characters

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

Password verification

When you provide a new password, you must confirm it by 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 again. No limit exists on the number of times you are allowed to update the password.

Password display masking

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

Read-Only and Read-Write passwords must be different

The RO and RW passwords cannot be the same.

Applicable passwords

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

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

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

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

Enabling and disabling password security

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

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

When password security is disabled, the following occurs:

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

Important:

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

Default passwords

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

HTTP port number change

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

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

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 3600 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

Configuring and managing security using CLI

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

Setting the system user name and password

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the username and password with the following command:

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

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

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

Variable definitions

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

Important:

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

Setting the password for selected types of access using CLI

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

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

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

Important:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the password for selected access or a specific authentication type by using the following commands:

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

Variable definitions

Variable	Value
read-only | read-write	Modify the read only password or the read/write password.
<password>	Enter your password. **Important:** This parameter is not available when Password Security is enabled, in which case the switch prompts you to enter and confirm the new password.
serial | telnet	Modify the password for serial console access or for Telnet access.
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 authentication for serial console or Telnet access. • tacacs: uses TACACS+ authentication, authorization, and accounting (AAA) services for serial console or Telnet access.

Enabling or disabling password security using CLI

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To enable password security, enter the following command:

   ```
   password security
   ```

   OR

   To disable password security, enter the following command:

   ```
   no password security
   ```

Displaying the security

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the prompt, enter the following command:

   ```
   show cli password
   ```

   You can view the authentication using the following command:

   ```
   show cli password type
   ```

Displaying the status of password security on the switch

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show password security
   ```

Example

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

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

Configuring the number of password logon attempts

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

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

   Note:

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

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

Configure 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.

Displaying the port number of the HTTP port

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show http-port
   ```

Example

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

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

Setting the HTTP port number

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

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

   OR

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

   ```
   default http-port
   ```

Viewing serial console port status

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show serial-console
   ```

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

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

Example

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

Variable definitions

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

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

Disabling USB ports

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

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

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

Variable definitions

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

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

Enabling USB ports

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

3. Enable USB ports on a stand-alone switch:

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

Variable definitions

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

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

Viewing USB port status

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

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

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

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

Variable definitions

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

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

Displaying Telnet access settings

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

Before you begin

To access CLI remotely, the management port must have an assigned IP address and remote access must be enabled.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show telnet-access
```

Example

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

```
Switch#show telnet-access
TELNET Access:       Enabled
Login Timeout:       1 minute(s)
Login Retries:       3
Inactivity Timeout:  15 minute(s)
Event Logging:       All
Allowed Source IP Address  Allowed Source Mask
-------------------------  ------------------
1  0.0.0.0                  0.0.0.0
2  255.255.255.0            255.255.255.0
3  255.255.255.0            255.255.255.0
4  255.255.255.0            255.255.255.0
5  255.255.255.0            255.255.255.0
6  255.255.255.0            255.255.255.0
7  255.255.255.0            255.255.255.0
8  255.255.255.0            255.255.255.0
9  255.255.255.0            255.255.255.0
10 255.255.255.0            255.255.255.0
11 255.255.255.0            255.255.255.0
12 255.255.255.0            255.255.255.0
13 255.255.255.0            255.255.255.0
14 255.255.255.0            255.255.255.0
15 255.255.255.0            255.255.255.0
----More (q=Quit, space/return=Continue)----
```

Configuring Telnet connections

Before you begin

To access CLI remotely, the management port must have an assigned IP address and remote access must be enabled.

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

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

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

Variable definitions

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

Variable	Value
enable | disable	Enables or disables Telnet connections.
login-timeout *<0–10>*	Specifies the time in minutes that you want to wait between an initial Telnet connection and acceptance of a password before closing the Telnet connection; enter an integer between 0 and 10. Zero (0) is used to indicate no timeout.
retry *<1–100>*	Specifies the number of times that the user can enter an incorrect password before closing the connection; enter an integer between 1 and 100.
inactive-timeout *<0–60>*	Specifies in minutes how long to wait before closing an inactive session; enter an integer between 0 and 60.
logging *{none|access|failures|all}*	Specifies what types of events you want to save in the event log: • **all**—Save all access events in the log: - Telnet connect—indicates the IP address and access mode of a Telnet session. - Telnet disconnect—indicates the IP address of the remote host and the access mode, due to either a log off or inactivity. - Failed Telnet connection attempts—indicates the IP address of the remote host that is not on the list of allowed addresses, or indicates the IP address of the remote host that did not supply the correct password. • **none**—No Telnet events are saved in the event log. • **access**—Connect and disconnect events are saved in the event log. • **failure**—Only failed Telnet connection attempts are saved in the event log.
source-ip *[<1–50> <A.B.C.D> | <51–100 <WORD>]*	Up to 50 IPv4 address/mask pairs (1–50) and 50 IPv6 address/prefix pairs (51–100) are supported. Specify the source IP addresses from which the connections are allowed: • Enter the IPv4 addresses as a mask from 1 to 50 and an IP address in the format A.B.C.D. • Enter the IPv6 addresses from 51–100 with a description.

Table continues…

Variable	Value
	Important: These are the same source IP addresses as in the IP Manager list. For more information about the IP Manager list, see Configuring the IP Manager list for IPv4 addresses using CLI on page 47 and Configuring the IP Manager list for IPv6 addresses using CLI on page 48.

Disabling Telnet access

Before you begin

To access CLI remotely, the management port must have an assigned IP address and remote access must be enabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

Variable	Value
source-ip *<1–50>* | *<51–100>*	Disables the Telnet access. When you do not use the optional parameter, the source-ip list is cleared, meaning that the 1st index is set to 0.0.0.0./0.0.0.0. and the 2nd to 100th indexes are set to 255.255.255.255/255.255.255.255. When you do specify a source-ip value, the specified pair is set to 255.255.255.255/255.255.255.255. • Specify <1–50> to select the address/mask pair to be disabled. • Specify <51–100> to select the IPv6 address/prefix to be disabled. **Important:** These are the same source IP addresses as in the IP Manager list. For more information about the IP Manager list, see Configuring the IP

Variable	Value
	Manager list for IPv4 addresses using CLI on page 47 and Configuring the IP Manager list for IPv6 addresses using CLI on page 48.

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).

Setting the switch HTTP/HTTPS port using EDM

Use the following procedure to configure HTTP/HTTPS port parameters for the switch:

Procedure steps

1. From the navigation tree, double-click **Security**.
2. In the Security tree, double-click **General**.
3. On the **Http/Https** tab, configure the HTTP/HTTPS parameters as required.
4. On the toolbar, click **Apply**.

Field Descriptions

The following table describes the fields of Http/Https tab.

Name	Description
HttpPort	Specifies a value for the switch HTTP port, ranging from 1024 to 65535. The default value is 80.
HttpsPort	Specifies a value for the switch HTTPS port, ranging from 1024 to 65535. The default value is 443.
SecureOnly	Configures the Web server to respond to HTTPS only, or both HTTPS and HTTP client browser requests. **Note:** If you configure the Web server to respond to HTTPS client browser requests only, all existing non-secure connections with the browser are terminated.

Configuring general switch security using EDM

Use this procedure to configure general switch security.

Procedure

1. In the navigation tree, double-click **Security** to open the Security tree..
2. From the Security tree, click **MAC Security**.
3. In the work area, click the **Mac Security** tab.
4. Configure switch security parameters as required.
5. On the toolbar, click **Apply**.

MAC Security Tab Field Descriptions

Use the data in the following table to use the **MAC Security** tab.

Name	Description
AuthSecurityLock	If this parameter is listed as *locked*, the agent refuses all requests to modify the security configuration. Entries also include: • **other** • **notlocked**
AuthCtlPartTime	This value indicates the duration of the time for port partitioning in seconds. The default is zero. When the value is zero, the port remains partitioned until it is manually enabled.
SecurityStatus	Indicates whether or not the switch security feature is enabled.
SecurityMode	Mode of switch security. Entries include: • **macList**: Indicates that the switch is in the MAC-list mode. You can configure more than one MAC address for each port. • **autoLearn**: Indicates that the switch learns the first MAC address on each port as an allowed address of that port.
SecurityAction	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 any security assigned to it, or the security feature is turned off. • **trap**: Listed trap. • **partitionPort**: Port is partitioned.

Table continues…

Name	Description
	• **partitionPortAndsendTrap**: Port is partitioned, and traps are sent to the trap receiver. • **daFiltering**: Port filters out the frames where the destination address field is the MAC address of the unauthorized station. • **daFilteringAndsendTrap**: Port filters out the frames where the desitnation address field is the MAC address of unauthorized station. Traps are sent to trap receivers. • **partitionPortAnddaFiltering**: Port is partitioned and filters out the frames with the destination address field is the MAC address of unauthorized station. • **partitionPortdaFilteringAndsendTrap**: Port is partitioned and filters out the frames where the destination address field is the MAC address of the unauthorized station. Traps are sent to trap receivers.
CurrNodesAllowed	Current number of entries of the nodes allowed in the AuthConfig tab.
MaxNodesAllowed	Maximum number of entries of the nodes allowed in the AuthConfig tab.
PortSecurityStatus	Set of ports for which security is enabled.
PortLearnStatus	Set of ports where autolearning is enabled.
CurrSecurityLists	Current number of entries of the Security listed in the SecurityList tab.
MaxSecurityLists	Maximum entries of the Security listed in the SecurityList tab.
AutoLearningAgingTime	Specifies the lifetime (in minutes) for MAC addresses that are learned automatically. Values range from 0 to 65535. The default value is 0. A value of 0 specifies that MAC addresses do not age out.
AutoLearningSticky (sticky-mac)	When selected, the learning mechanism used is the same as when auto-learning is enabled, with the exception that: • when the Sticky MAC feature is enabled, migration and auto-deletion on link-down are blocked and the addresses are not aged out • when Sticky mode is enabled, the aging timer is automatically set to zero • Sticky MAC addresses are saved into NVRAM config file and ASCII files

Table continues…

Name	Description
	• administrative removal of sticky addresses is possible

Important:

You cannot assign a port or ports to the PortLearnStatus field if you have enabled AutoLearn for the port or ports.

Adding ports to a security list using EDM

Use this procedure to add ports to the security list to insert new port members into a security list.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **MAC Security**.
3. In the work area, click the **SecurityList** tab.
4. On the toolbar, click **Insert**.
5. Perform one of the following:
   - In the **SecurityListIndx** box, accept the default sequential security list number provided by the switch.
   - Enter a number for the security list.
6. Click the ellipsis **(...)** for **SecurityListMembers** and do one of the following:
   - In the **SecurityListMembers** select ports to add to the security list.
   - Click **All** to select all ports.
7. Click **Ok**.
8. Click **Insert** to return to the SecurityList tab.
9. On the toolbar, click **Apply**.

SecurityList Tab Field Descriptions

Use the data in the following table to use the **SecurityList** tab.

Name	Description
SecurityListIndx	An index of the security list. This corresponds to the SecurityList field into AuthConfig tab.
SecurityListMembers	The set of ports that are currently members in the Port list.

Deleting ports from a security list using EDM

Use this procedure to delete ports from a security list.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **MAC Security**.
3. In the work area, click the **SecurityList** tab.
4. Click rows in the table to delete.
5. On the tool bar, click **Delete**.
6. Click **Yes** to delete the selections or click **No** to return to the SecurityList tab without deleting any entries.

SecurityList Tab Field Descriptions

Use the data in the following table to use the **SecurityList** tab.

Name	Description
SecurityListIndx	A numerical identifier for a security list. Values range from 1 to 32.
SecurityListMembers	Defines the security list port members.

Configuring AuthConfig list using EDM

The AuthConfig list contains a list of boards, ports and MAC addresses that have the security configuration. An SNMP SET PDU for a row in the tab requires the entire sequence of the MIB objects in each entry to be stored in one PDU, otherwise, the switch returns a GENERR return-value.

Adding entries to the AuthConfig list using EDM

Use this procedure to add entries to the AuthConfig list.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **MAC Security**.
3. In the work area, click the **AuthConfig** tab.
4. On the tool bar, click **Insert** to open the Insert AuthConfig window.
5. Type a value in the **BrdIndx** field.
6. Type a value in the **PortIndx** field.

7. Type a value in the **MACIndx** field.
8. Select the **AutoLearningSticky (sticky-mac)** check box to enable Sticky MAC address, or clear the check box to disable.

   Important:

   Extreme Networks recommends you to disable autosave if you enable Sticky MAC address.
9. Select the **AccessCtrlType** check box to enable a MAC address on multiple ports, or clear the check box to disable.
10. Click **Insert** .
11. Type a value in the **SecureList** field.
12. On the toolbar, click **Apply**.

AuthConfig Tab Field Descriptions

Use the data in the following table to use the **AuthConfig** tab.

Name	Description
BrdIndx	Index of the slot that contains the board on which the port is located. If you specify SecureList, this field must be zero.
PortIndx	Index of the port on the board. If you specify SecureList, this field must be zero.
MACIndx	An index of MAC addresses that are designated as allowed (station).
AutoLearningSticky (sticky-mac)	Enables or disables Sticky MAC. Sticky MAC can store automatically learned MAC addresses across switch reboots and secure MAC addresses to a specified port. **Note:** If AutoLearningSticky is enabled, you cannot modify AccessCtrolType and SecureList.
AccessCtrlType	Displays the node entry as node allowed. A MAC address can be allowed on multiple ports.
SecureList	The index of the security list. This value is meaningful only if BrdIndx and PortIndx values are zero. For other board and port index values, this index must also have a value of zero. The corresponding MAC Address of this entry is allowed or blocked on all ports of this port list.
Source	Indicates the source MAC address.
Lifetime	Indicates the time period that the system stores information before it deletes the information.

Deleting entries from the AuthConfig list using EDM

Use this procedure to remove entries from the AuthConfig list for boards, ports and MAC addresses that have the security configuration.

Procedure

1. In the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **MAC Security**.
3. In the work area, click the **AuthConfig** tab.
4. Click a list entry.
5. On the tool bar, click **Delete**.
6. Click **Yes**.

Viewing AuthStatus information using EDM

Use this procedure to view AuthStatus information about the current security status of a port. The information includes actions to be performed when an unauthorized station is detected.

Procedure

1. In the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **MAC Security**.
3. In the work area, click the **AuthStatus** tab.

AuthStatus Tab Field Descriptions

Use the data in the following table to use the **AuthStatus** tab.

Name	Description
AuthStatusBrdIndx	The index of the board. This corresponds to the index of the slot that contains the board if the index is greater than zero.
AuthStatusPortIndx	The index of the port on the board. This corresponds to the index of the last manageable port on the board if the index is greater than zero.
AuthStatusMACIndx	The index of MAC address on the port. This corresponds to the index of the MAC address on the port if the index is greater than zero.
CurrentAccessCtrlType	Displays whether the node entry is the `node allowed` or `node blocked` type.

Table continues…

Name	Description
CurrentActionMode	A value representing the type of information contained, including: • **noAction**: Port does not have any security assigned to it, or the security feature is turned off.. • **partitionPort**: Port is partitioned. • **partitionPortAndsendTrap**: Port is partitioned and traps are sent to the trap receiver. • **Filtering**: Port filters out the frames where the destination address field is the MAC address of the unauthorized station. • **FilteringAndsendTrap**: Port filters out the frames where the destination address field is the MAC address of the unauthorized station. Traps are sent to the trap receiver. • **sendTrap**: A trap is sent to the trap receiver(s). • **partitionPortAnddaFiltering**: Port is partitioned and filters out the frames where the destination address field is the MAC address of the unauthorized station • **partitionPortdaFilteringAndsendTrap**: Port is partitioned and filters out the frames where the destination address field is the MAC address of the unauthorized station. Traps are sent to trap receiver(s).
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 this procedure to view authorization violation information that includes a list of boards and ports where network access violations have occurred, and the MAC addresses of violators.

Procedure

1. In the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **MAC Security**.
3. In the work area, click the **AuthViolation** tab.

AuthViolation Tab Field Descriptions

Use the data in the following table to use the **AuthViolation** tab.

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

Chapter 4: IP Manager

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

With the IP Manager, you can do the following:

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

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

Important:

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

Configuring IP Manager using CLI

This section provides procedures to configure IP Manager using CLI.

Configuring IP Manager

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   [no] ipmgr {snmp | ssh | telnet | web}
   ```

Variable definitions

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

Variable	Value
snmp	Enables the IP Manager list check for SNMP including Enterprise Device Manager.
ssh	Enables the IP Manager list check for SSH access.
telnet	Enables the IP Manager list check for telnet access.
web	Enables the IP Manager list check for web-based management system.

Configuring the IP Manager list for IPv4 addresses

Use the following procedure to configure the IP Manager list to specify the source IP addresses or address ranges, with list IDs between 1 and 50, that have access to the switch when IP Manager is enabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   ipmgr source-ip <listID> <ipv4addr> [mask <mask>]
   ```

Variable definitions

The following table describes the parameters for the **ipmgr source-ip** command.

Variable	Value
<ipv4addr>	Specifies the source IP address from which access is allowed. Enter the IP address either as an integer or in dotted-decimal notation.
<listID>	Specifies an integer in the range 1 to 50 for IPv4 entries and 51–100 for IPv6 entries that uniquely identifies the entry in the IP Manager list.
mask *<mask>*	Specifies the subnet mask from which access is allowed. Enter the IP mask in dotted-decimal notation.

Configuring the IP Manager list for IPv6 addresses

Use the following procedure to configure the IP Manager list to specify the source IP addresses or address ranges, with list IDs between 51 and 100, that have access to the switch when IP Manager is enabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   ipmgr source-ip <listID> <ipv6addr/prefix>
   ```

Variable definitions

The following table describes the parameters for the **`ipmgr source-ip`** command.

Variable	Value
<ipv6addr/prefix>	Specifies the source IPv6 address and prefix from which access is allowed.
<listID>	Specifies an integer in the range 1 to 50 for IPv4 entries and 51–100 for IPv6 entries that uniquely identifies the entry in the IP Manager list.

Removing IP Manager list entries

Use the following procedure to remove IP Manager list entries to deny access to the switch for specified source IP addresses or address ranges.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   no ipmgr source-ip [<listID>]
   ```

   The command sets both the IP address and mask for the specified entry to 255.255.255.255 for IPv4 entries, and to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF/128 for IPv6 entries.

Variable definitions

The following table describes the parameters for the **no ipmgr source-ip** command.

Variable	Value
<listID>	Specifies an integer in the range 1–50 for IPv4 addresses and range 51–100 for IPv6 addresses, that uniquely identifies the entry in the IP Manager list. If you do not specify a <listID>, the command resets the entire list to factory defaults.

Displaying the IP Manager configuration

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show ipmgr
   ```

Example

The following figure provides a sample of the **show ipmgr** command for IPv4 addresses (1–50).

```
Switch(config)#show ipmgr
TELNET Access: Enabled
SNMP Access:   Enabled
WEB Access:    Enabled
TELNET IP List Access Control:  Enabled
SNMP IP List Access Control:    Enabled
WEB IP List Access Control:     Enabled
Allowed Source IP Address   Allowed Sourced Mask
-------------------------   --------------------
1   0.0.0.0                   0.0.0.0
2   255.255.255.0             255.255.255.0
3   255.255.255.0             255.255.255.0
4   255.255.255.0             255.255.255.0
5   255.255.255.0             255.255.255.0
6   255.255.255.0             255.255.255.0
7   255.255.255.0             255.255.255.0
8   255.255.255.0             255.255.255.0
9   255.255.255.0             255.255.255.0
10  255.255.255.0             255.255.255.0
11  255.255.255.0             255.255.255.0
12  255.255.255.0             255.255.255.0
13  255.255.255.0             255.255.255.0
14  255.255.255.0             255.255.255.0
----More   (q=Quit, space/return=Continue) ----
```

The following figure provides a sample of the **show ipmgr** command for IPv6 addresses (51–100).

```
Allowed Source IPv6 Address
-----------------------------------
51   ::/0
```

```
52  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
53  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
54  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
55  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
56  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
57  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
58  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
59  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
60  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
61  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
62  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
63  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
64  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
----More   (q=Quit, space/return=Continue) ----
```

Chapter 5: 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 supports the following features:

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

An SSL certificate is generated when:

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

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

On deletion, the certificate in NVRAM is also deleted.

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

Secure versus non-secure mode

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

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

secure mode, the Web server listens on TCP port 80, by default, and responds only to HTTP client browser requests. All existing secure connections with the browser are closed down.

The TCP port can be designated as any number from 1024 to 65535.

SHA-2 Support for SSL Certificates

In Release 6.0.0 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 6.0.0 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 6.0.0 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 55.

Configuring SSL using the CLI

This section provides procedures to configure SSL to secure a Web management interface using CLI.

Enable or Disable 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
   ```

Create or Delete 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
   ```

View 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.

View 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
```

Regenerate 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 this procedure to configure Secure Socket Layer (SSL) to provide your network with a secure Web management interface.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, double-click **SSH/SSL**.
3. In the work area, click the **SSL** tab.
4. Configure SSL parameters as required.
5. On the toolbar, click **Apply**.

SSL Tab Field Descriptions

Use the data in the following table to use the **SSL** tab.

Name	Description
Enabled	Enables or disables SSL.
CertificateControl	Enables the creation and deletion of SSL certificates. • **create**: creates an SSL certificate • **delete**: deletes an SSL certificate. • **other**: results in a wrongValue error
CertificateExists	Indicates if a valid SSL certificate is created. • **true**: a valid SSL certificate is created • **false**: a valid SSL certificate is not created or the certificate has been deleted
CertificateControlStatus	Indicates the status of the most recent attempt to create or delete a certificate. • **inProgress**: the operation is not yet completed • **success**: the operation is complete • **failure**: the operation failed

Table continues…

Name	Description
	• **other**: the s5AgSslCertificateControl object was never set
ServerControl	Resets the SSL server. Values are reset and other. The default is other.

Important:

You cannot reset the SSL server while creating the SSL certificate.

Chapter 6: 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 File Transfer Protocol (SFTP over SSH)

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

The following SFTP features are supported:

- a binary configuration file upload to an SFTP server
- a binary configuration file download from an SFTP server
- DSA key authentication
- RSA key authentication
- password authentication
- host key generation
- 1024-bit DSA-key use for authentication. The DSA key range is 512-1024 and is multiple of 64.
- 2048-bit RSA-key use for authentication. The RSA key range is 1024-2048 and is multiple of 128.

SSH enhancement to support RSA

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

Secure Shell protocol configuration using CLI

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

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

Displaying SSH information

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Example

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

```
Switch#show ssh global
Active SSH Sessions     :  0
Version                 :  Version 2 only
Port                    :  22
Authentication Timeout  :  60
DSA Authentication      :  True
RSA Authentication      :  True
Password Authentication :  True
Auth Retries            :  3
Auth Key TFTP Server    :  192.0.2.1
DSA Auth Key File Name  :
RSA Auth Key File Name  :
DSA Host Keys           :  Exist
RSA Host Keys           :  Exist
Enabled                 :  False
```

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

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

Variable definitions

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

Variable	Value
download-auth-key	Displays authorization key and TFTP server IP address

Table continues…

Variable	Value
global	Displays general SSH settings.
session	Displays SSH session info.

Configuring SSH

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the prompt, enter the following command:

   ```
   ssh
   ```

3. Disable SSH for the switch:

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

Generating the DSA host keys

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

Note:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

3. Delete the switch SSH DSA host key:

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

Generating the SSH RSA host key

Use the following procedure to generate the RSA host keys.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

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

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

Downloading DSA or RSA authentication keys

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

Variable	Value
address <*A.B.C.D*> <*WORD*>	Specifies the IP address of the TFTP server. • A.B.C.D—specifies the IP address • WORD—specifies the IPv6 address
dsa	Download SSH DSA auth key.
key-name <*WORD*>	Specifies the TFTP filename.
rsa	Download the SSH RSA auth key.
unit <*1–8*>	Specifies the unit number in a stack from which to download the SSH auth key using USB.

Deleting the SSH DSA authentication key

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Deleting the SSH RSA authentication key

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Enabling user log-on with an SSH DSA key

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   [default] ssh dsa-auth
   ```

3. Disable user log-on with SSH DSA key authentication:

   ```
   no ssh dsa-auth
   ```

Variable definitions

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

Variable	Value
no	Disables DSA authentication.

Enabling user log-on with an SSH RSA key

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   [default] ssh rsa-auth
   ```

3. Disable user log-on with SSH RSA key authentication:

   ```
   no ssh rsa-auth
   ```

Enabling user log-on with SSH password authentication

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the prompt, enter the following command:

   ```
   [default] ssh pass-auth
   ```

3. Disable user log-on using the SSH password authentication method:

   ```
   no ssh pass-auth
   ```

Disabling SNMP and Telnet With SSH

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   ssh secure [force]
   ```

Variable definitions

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

Variable	Value
force	Skips the confirmation step.

Configuring the TCP port for SSH daemon

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

3. Configure the default TCP port for the SSH daemon:

   ```
   default ssh port
   ```

Variable definitions

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

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

Configuring the timeout value for session authentication

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

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

   ```
   default ssh timeout
   ```

Variable definitions

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

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

Configuring and clearing the SSH banner

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

Note:

The maximum size of the SSH banner is 1564 characters.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

3. Display the banner:

   ```
   show ssh banner
   ```

4. (Optional) Clear the SSH banner:

   ```
   clear ssh banner
   ```

Example

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

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

Variable definitions

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

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

Configuring SSH retry

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

3. (Optional) Set SSH retries to default value:

   ```
   default ssh retries
   ```

Secure Shell Client configuration

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

Opening and closing an SSH session involves three actions:

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

Configuring SFTP authentication for SSH Client

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Configure the SFTP authentication method the SSH Client uses for transferring files:

```
sshc authentication {dsa | password | rsa}
```

3. Configure the SFTP authentication method SSH Client to the default of DSA:

```
default sshc authentication
```

OR

```
no sshc authentication
```

Variable definitions

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

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

Generating an SSHC DSA host key

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
sshc dsa-host-key [force]
```

3. Delete the public or private DSA host keys from NVRAM:

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

Variable definitions

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

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

Generating an SSHC RSA host key (public and private)

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   sshc rsa-host-key [force]
   ```

3. Delete the public or private DSA host keys from NVRAM

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

Variable definitions

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

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

Configuring SSHC DSA host key size

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Configuring SSHC RSA host key size

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

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
sshc rsa-key <1024–2048>
```

Variable definitions

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

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

Configuring the SSHC port

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
sshc port <portnumber>
```

Variable definitions

The following table describes the parameters for the **sshc port** command.

Variable	Value
<portnumber>	Specifies the TCP port as a value from 1–65535. The default port is 22.

Viewing Secure File Transfer Protocol (SFTP)

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
show sshc
```

Example

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

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

```
    RSA Auth Key            :  Exist
    RSA key size            :  2048

SFTP:
    DSA Authentication      :  True
    RSA Authentication      :  False
    Password Authentication :  False
    User Name               :  admin
    SFTP Server Address     :  0.0.0.0
    Port                    :  22
```

Variable definitions

The following table describes the parameters for the **show sshc** command.

Variable	Value
Version	Displays the SSH version. Option 2 is the only valid option.
Port	Displays the SSH connection port. RANGE: 1 to 65535 DEFAULT: 22
Authentication Timeout	Displays the timeout interval in seconds. DEFAULT: 30
DSA Authentication	Displays the DSA Authentication state. DEFAULT: True
RSA Authentication	Displays the RSA Authentication state. DEFAULT: True
User Name	Displays the user name. DEFAULT: admin
SFTP Server Address	Displays the SFTP server IP address.
DSA Auth Key	Displays the authentication key if it is configured.
DSA key size	Displays the DSA key size as an integer (multiple of 64). RANGE: 1024 to 1024 DEFAULT: 1024
RSA Auth Key	Displays the authentication key if it is configured.
RSA key size	Displays the RSA key size as an integer (multiple of 128). RANGE: 1024 to 2048 DEFAULT: 2048

Uploading a config file to an SFTP server

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   copy config sftp address <A.B.C.D | WORD> filename [username <WORD>
   password <WORD>]
   ```

   Notes:

   - If you enter the **address** parameter, the system saves it as the default values.
   - If you do not enter the password and username, the command fails.
   - If you disable password authentication (that is, you enabled DSA key authentication), the command parameters **password** and **username** are optional and are not saved.

Variable definitions

The following table describes the parameters for the **`copy config sftp`** command.

Variable	Value
address <A.B.C.D | WORD >	Specifies the address of the SFTP server as follows: • A.B.C.D is the IPv4 address format • WORD is the IPv6 address format
filename <WORD>	Specifies the configuration file name.
password <WORD>	Specifies the password.
username <WORD>	Specifies the username

Downloading a config file from an SFTP server

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   copy sftp config address <A.B.C.D | WORD> filename [username <WORD>
   password <WORD>]
   ```

   Notes:

   - If you enter the **address** and **filename** parameters, the system saves them as the default values.

- If you enable password authentication (that is, you disabled the DSA key authentication), the command parameters **password** and **username** are required.
- If you do not enter the password and username, the command fails.
- If you disable password authentication (that is, you enabled DSA key authentication), the command parameters **password** and **username** are optional and are not saved.

Variable definitions

The following table describes the parameters for the **`copy sftp config address`** command.

Variable	Value
<A.B.C.D | WORD>	Specifies the address of the SFTP server as follows: • A.B.C.D is the IPv4 address format • WORD is the IPv6 address format
filename <WORD>	Specifies the configuration file name.
password <WORD>	Specifies the password.
username <WORD>	Specifies the username.

Secure Shell Protocol Configuration using EDM

This section provides procedures to configure Secure Shell (SSH) protocol using EDM.

Configuring the Secure Shell protocol using EDM

Use this procedure to configure the Secure Shell (SSH) protocol to provide secure access to the switch.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, double-click **SSH/SSL**.
3. In the work area, click the **SSH** tab.
4. Configure SSH parameters as required.
5. On the toolbar, click **Apply**.

SSH Tab Field Descriptions

Use the data in the following table to use the **SSH** tab.

Name	Description
Enable	Indicates the SSH status. Values include: • **false**: Disabled • **true**: Enabled • **secure**: SSH enabled, turns off all remote access, takes effect after a reboot Default is false.
Version	Indicates the SSH version. The default is v2only.
Port	Indicates the SSH connection port. Value range of 1 to 65535, default is 22.
Timeout	Indicates the SSH connection timeout in seconds. Value range of 1 to 120, default is 60.
KeyAction	Indicates the SSH key action. Values include: • **generateDsa** • **generateRsa** • **deleteDsa** • **deleteRsa**
DsaAuth	Enables or disables SSH with DSA public key authentication. The default is enabled.
PassAuth	Enables or disables SSH with password authentication. The default is enabled.
DsaHostKeyStatus	Indicates the current status of the SSH DSA host key: • **notGenerated**: DSA host key has not yet been generated. • **generated**: DSA host key is generated. • **generating**: DSA host key is currently being generated.
RsaAuth	Enables or disables SSH with RSA public key authentication. The default is enabled.
RsaHostKeyStatus	Indicates the current status of the SSH DSA host key: • **notGenerated**: RSA host key has not yet been generated. • **generated**: RSA host key is generated. • **generating**: RSA host key is currently being generated.

Table continues…

Name	Description
TftpServerInetAddressType	Indicates the type of address stored in the TFTP server. Values include: • **IPv4** • **IPv6** The default is IPv4.
TftpServerInetAddress	Specifies the IP address of TFTP server for all TFTP operations.
TftpFile	Indicates the name of the file for the TFTP transfer.
TftpAction	Indicates the SSH public keys that are set to initiate a TFTP download. Values include: • **none** • **downloadSshDsaPublicKeys** • **deleteSshDsaAuthKey** • **downloadSshRsaPublicKeys** • **deleteSshRsaAuthKey** The default is none
TftpResult	Indicates the retrieved value of the TFTP transfer. Values include: • **none** • **success** • **transferError**

Viewing SSH Sessions information using EDM

Use this procedure to display currently active SSH sessions.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, double-click **SSH**.
3. In the work area, click the **SSH Sessions** tab.

SSH Sessions Tab Field Descriptions

Use the data in the following table to use the **SSH Sessions** tab.

Name	Description
SshSessionInetAddressType	Indicates the type of IP address of the SSH client that opened the SSH session.
SshSessionInetAddress	Indicates the IP address of the SSH client that opened the SSH session.

Configuring an SSH Client

Use this procedure to configure and manage a Secure Shell (SSH) Client.

Procedure

1. In the navigation tree, double-click **Security**.
2. In the Security tree, click **SSH/SSL**.
3. In the work area, click the **SSHC/SFTP** tab.
4. Configure SSHC parameters as required.
5. Click **Apply**.

SSHC/SFTP Tab Field Descriptions

Use the data in the following table to use the **SSHC/SFTP** tab.

Name	Description
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 DSA host key. • **generateDsaForce**: generates a new, active DSA key, even in the presence of an existing DSA key. • **generateRsaForce**: generates a new, active RSA key, even in the presence of an existing RSA key.
KeyFileName	Speicifies the SSH Client host key file name.

Table continues…

Name	Description
TftpAction	Specifies the type of SSH Client authentication key to upload using TFTP. Values include: • **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
TftpServerInetAddressType	Specifies whether the IP address is IPv4 or IPv6.
TftpServerInetAddress	Specifies the IP address of the TFTP server.
DsaKeySize	Specifies the DSA key size. Values range from 512 to 1024. Default value: 512.
RsaKeySize	Specifies the RSA key size. Values range from 1024 to 2048. Default value: 1024.
DSAHostKeyStatus	Indicates the current status of the SSH Client DSA host key. Values include: • 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. Default value: 22.
DsaAuthentication	When selected, enables SFTP DSA authentication for SSH Client (default).
RsaAuthentication	When selected, enables SFTP password authentication for SSH Client.
PasswordAuthentication	When selected, enables SFTP RSA authentication for SSH Client.
SftpServerInetAddressType	Specifies whether the IP address is IPv4 or IPv6.
SftpServerInetAddress	Specifies the IP address of the SFTP server.
UserName	Specifies the user name.
SftpServerPassword	Specifies the password for the SFTP server.

Table continues…

Name	Description
Confirm SftpServerPassword	Confirm the password for the SFTP server.

Chapter 7: 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

Use the MAC address-based security to set up network access control based on source MAC addresses of authorized stations. You can perform the following activities:

- Create a list of up to 448 MAC addresses and specify which addresses are authorized to connect to your switch. The 448 MAC addresses can be configured within a single standalone switch, or they can be distributed in any order among the units in a single stack configuration.
- Specify which switch port each MAC address can access.

  The options for allowed port access include NONE, ALL, and single or multiple ports specified in a list.
- Specify optional switch actions if the software detects a security violation.

  The response can be to send a trap, turn on destination address (DA) filtering, disable a specific port, or a combination of these three options.

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

MAC address-based security autolearning

The MAC address-based security autolearning feature provides the ability to add allowed MAC addresses to the MAC Security Address Table automatically without user intervention. MAC address-based security autolearning contains the following features:

- You can specify the number of addresses to learn on the ports to a maximum of 25 addresses for each port. The switch forwards traffic only for those MAC addresses statically associated with a port or learned with the autolearning process.
- You can configure an aging timer, in minutes, after which autolearned entries are refreshed in the MAC Security Address Table. If you set the aging time value to 0, the entries never age out.

To force relearning of entries in the MAC Security Address Table you must reset learning for the port.

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

Sticky MAC address

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

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

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.

Block subsequent MAC authentication

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

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

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

MultiVlan Disabled:

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

EAP clients are blocked in the following situations:

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

Note:

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

Non-EAP clients are blocked in following situations:

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

Note:

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

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

MultiVlan Enabled:

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

EAP clients are blocked in the following situations:

- EAP client comes without any VLAN
- EAP client comes with a VLAN that does not exist on the switch

- EAP client comes with a VLAN different from the one specified by the first EAP client present on port
- “use-radius-assignment-vlan” is disabled on port
- EAP client comes with a VLAN for Non-EAP clients

Non-EAP clients are blocked in the following situations:

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

Note:

No PVID changes.

MAC Address-Based Security Configuration using CLI

This section describes the procedures you can use to configure MAC address-based security using CLI.

Configuring MAC address filter-based security using CLI

Displaying MAC address security settings

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

Before you begin

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Example

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

```
Switch(config)#show mac-security config
MAC Address Security: Disabled
```

```
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Disabled
MAC Auto-Learning Age-Time: 60 minutes
MAC Auto-Learning Sticky Mode: Disabled
Current Learning Mode: Disabled
Learn by Ports: NONE
```

Variable definitions

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

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

Configuring MAC address security options

Use the following procedure to modify the BaySecure configuration.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

The following table describes the parameters for the command.

Variable	Value
auto-learning aging-time *<0-65535>*	Configures the maximum MAC address autolearn aging time. RANGE: 0 to 65535
disable|enable	Disables or enables MAC address-based security.

Table continues…

Variable	Value
filtering {enable|disable}	Enables or disables destination address (DA) filtering when an intrusion is detected.
intrusion-detect {enable|disable|forever}	Specifies the partitioning of a port when an intrusion is detected: • *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 *<0-65535>*	Temporary partition time in seconds. Default value is 0.
learning {enable|disable}	Specifies MAC address learning: • *enable*— enables learning by ports • *disable*— disables learning by ports **Important:** The MAC address learning enable command must be executed to specify learning ports.
learning-ports *<portlist>*	Specifies MAC address learning. Learned addresses are added to the table of allowed MAC addresses. Enter the ports you want to learn; this can be a single port, a range of ports, several ranges, all, or none.
mac-address-table	Adds addresses to the MAC security address table.
mac-da-filter	Adds or deletes MAC DA filtering addresses.
security-list	Modifies security list port membership.
snmp-lock {enable|disable}	Enables or disables a lock on SNMP write-access to the BaySecure MIBs.

Adding addresses to MAC security address table

Use the following procedure to assign either a specific port or a security list to the MAC address. This removes any previous assignment to the specified MAC address and creates an entry in the BaySecure table of allowed MAC addresses.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Assigning a list of ports to a security list

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Disabling MAC source address-based security

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   no mac-security
   ```

Disabling MAC address auto-learning aging time

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Clearing the MAC address security table

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

Variable	Value
address *<H.H.H>*	Enter the MAC address in the form of H.H.H
port *<portlist>*	Enter a list or range of port numbers.
security-list *<1–32>*	Enter the security list number.

Clearing the port membership of a security list

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Configuring MAC security for specific ports

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

Procedure

1. Enter Ethernet Interface Configuration mode:

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

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

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

   Note:

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

Variable definitions

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

Variable	Value
port *<portlist>*	Specifies the port numbers.
auto-learning|disable|enable|learning	Directs the specific port: • 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

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Important:

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

Configuring MAC address autolearning using CLI

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

Configuring MAC address auto-learning aging time

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

Variable	Value
<0–65535>	Specifies the aging time period in minutes. A value of 0 indicates an infinite aging time period.

Variable	Value
	DEFAULT: 60 minutes RANGE: 0 to 65535

Disabling MAC address auto-learning aging time

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Configuring MAC address auto-learning aging time to default

Use the following procedure to configure MAC address auto-learning aging time to default to configure the aging time for the MAC addresses automatically learned in the MAC security table. The default value is 60 minutes.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Enabling or disabling block subsequent MAC authentication

Note:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Note:

By default this feature is disabled.

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

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

OR

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

Viewing the current Sticky MAC address mode

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

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

```
show mac-security config
```

Example

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

```
Switch#config
Configuring from terminal or network [terminal]? terminal
Enter configuration commands, one per line.  End with CNTL/Z.
3524GT-PWR+(config)#show mac-security config
MAC Address Security: Disabled
MAC Address Security SNMP-Locked: Disabled
Partition Port on Intrusion Detected: Disabled
DA Filtering on Intrusion Detected: Disabled
MAC Auto-Learning Age-Time:  60 minutes
MAC Auto-Learning Sticky Mode: Disabled
Current Learning Mode: Disabled
Learn by Ports: NONE
```

Enabling Sticky MAC address mode

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

Before you begin

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

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Disabling Sticky MAC address mode

The default state is disabled.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

OR

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

Displaying all MACs

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

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display information on MACs for EAP sessions:

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

3. Display the summary of authenticated clients:

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

Example

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

```
Switch(config)#show eapol sessions

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

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

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

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


Switch(config)#show eapol summary

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


Switch(config)#show eapol summary verbose

                         Unit 1 Unit 2 Unit 3 Total
                         ------ ------ ------ -----
EAP Clients              :    2      0      0     2
NEAP Clients (total)     :    2      1      0     3
     Radius Clients      :    2      1      0     3
     User config Clients :    0      0      0     0
     Adac Clients        :    0      0      0     0
     Adac LLdp Clients   :    0      0      0     0
     Mhsa Clients        :    0      0      0     0
     Held Clients        :    0      0      0     0
DHCP Clients             :    1      0      0     1
Unauthenticated (total)  :    5      0      0     5
     Intruders           :    5      0      0     5
     Guests              :    0      0      0     0
```

```
    Fail Open           :    0       0       0      0
    Mhsa no limit       :    0       0       0      0
```

Variable definitions

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

Variable	Value
port <portmask>	Specifies the numeric slot/port format. Range: 1/1 to 8/50 or ALL If no port is specified, the default is ALL. If no parameter is specified, the default is show everything. If “non-eap” is without other parameters, all types of non-eap authenticated macs are shown, except when MHSA under no-limit flag is enabled. When “unauthenticated” is not followed by parameters, all unauthenticated macs are shown.
dhcp-phones	Displays MACs of DHCP Phones.
eap	Displays authenticated EAPOL sessions.
non-eap	Displays authenticated non-EAPOL clients.
radius	Displays non-EAPOL clients authenticated by RADIUS.
local	Displays locally authenticated non-EAPOL clients.
adac-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 autolearn using EDM

Use this procedure to configure automatic learning of MAC Addresses.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **MAC Security**.
3. In the work area, click the **AutoLearn**.
4. In the Enabled column, double-click the cell for a port.
5. From the list, select **true** or **false**.
6. In the MaxMacs column, double-click the cell for the port.
7. Enter a value from 1 to 25.
8. On the toolbar, click **Apply**.

AutoLearn Tab Field Descriptions

Use the data in the following table to use the **AutoLearn** tab.

Name	Description
Brd	The index of the board. This corresponds to the slot containing the board. The index is 1 when it is not applicable. This column is titled Unit if the switch is in a stack.
Port	Identifies the switch port number.
Enabled	Enables or disables the automatic learning of MAC addresses on the port. Values are true (enabled) and false (disabled).
MaxMacs	Defines the maximum number of MAC addresses the port can learn. Values range from 1 to 25.

Important:

You cannot enable AutoLearn if the port is a member of PortLearnStatus on the Mac Security tab. If you disable AutoLearn, the switch removes all automatically learned MAC addresses for the port or ports.

Chapter 8: EAPOL-based Security

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

EAPOL-based security fundamentals

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

An example follows to show how a switch reacts when it is configured with the EAPOL security feature and a new network connection:

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

The EAPOL-based security comprises of the following terms:

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

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

The authenticator PAE encapsulates the EAP through the RADIUS server packet and sends it to the authentication server. The authenticator server sends the packet in an exchange that occurs between the supplicant and authentication server. This exchange occurs when the EAP message is encapsulated to make it suitable for the destination of the packet.

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

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

EAPOL Security Configuration

EAPOL security lets you selectively limit access to the switch based on an authentication mechanism that uses Extensible Authentication Protocol (EAP) to exchange authentication information between the switch and an authentication server.

Important:

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

- User names
- Passwords
- VLAN IDs
- Port priority

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

Important:

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

EAPOL with Guest VLAN

Basic EAP (802.1X) Authentication supports Port Based User Access. At any time, only one user (MAC) can be authenticated on a port, and the port can be assigned to only one Port-based VLAN. Only the MAC address of the device or user that completed the EAP negotiations on the port has

access to that port for traffic. Any tagging of ingress packets are to the PVID of that port. This remains the default configuration.

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

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)

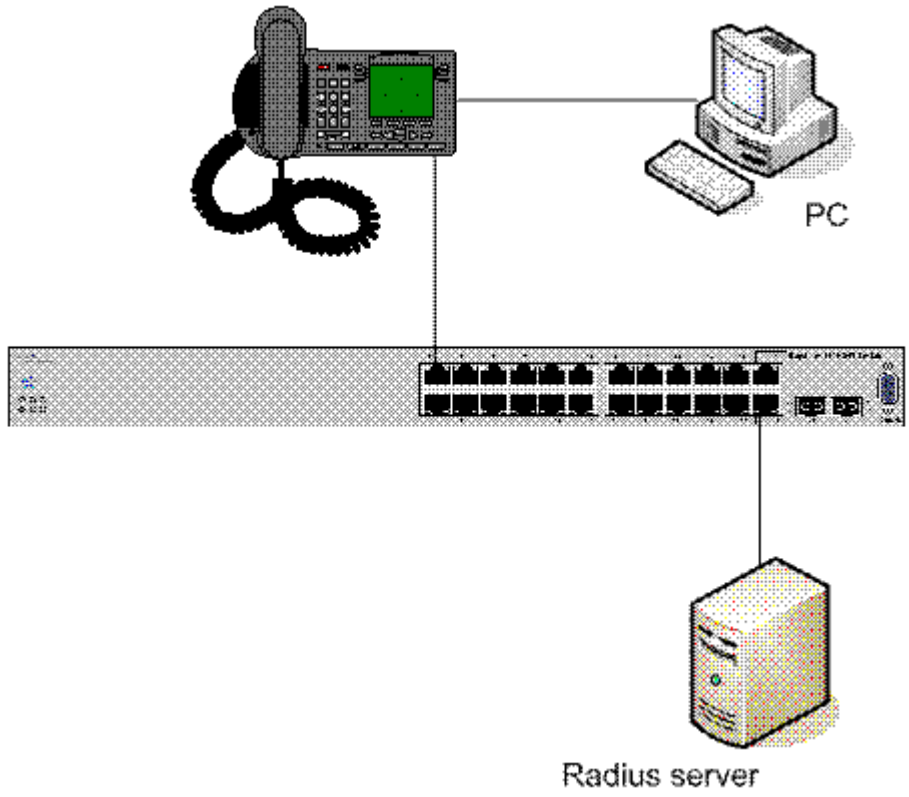

Figure 3: RADIUS-assigned VLAN in MHMA-MV mode

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, unicast 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.

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 all these VLANs.

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 enabled in the Global Configuration and Interface Configuration modes, for all switch ports.

Non-EAP IP Phone authentication

Non-EAP and ADAC non-EAP IP Phone authentication can be used for IP Phones that cannot authenticate with EAP. On an EAP capable IP Phone, EAP must be disabled to use non-EAP IP Phone authentication. DHCP must be enabled on the phone, because the switch examines the phone signature in the DHCP Discover packet sent by the phone.

802.1X or non-EAP with VLAN names

When you use the 802.1X or non-EAP with VLAN names functionality, the switch can match RADIUS assigned VLANs based on either the VLAN number or the VLAN name. Because the 802.1X or non-EAP with VLAN names mode is always enabled, you do not have to configure this feature. Prior to Release 5.0, a match occurred based on the VLAN number of the Tunnel- Private-Group-Id attribute returned by the RADIUS server. Beginning with Release 5.0, you can use the VLAN number or name to configure VLAN membership of EAP or non-EAP clients.

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

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

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

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

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

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

Non-EAP hosts on EAP-enabled ports

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

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

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

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

- EAPOL and authenticated non-EAPOL clients are allowed on the port at the same time. Authenticated non-EAPOL clients are hosts that satisfy one of the following criteria:
  - Host MAC address matches an entry in an allowed list preconfigured for the port.
  - Host MAC address is authenticated by RADIUS.
- Non-EAPOL hosts are allowed even if no authenticated EAPOL hosts exist on the port.
- When a new host is seen on the port, non-EAPOL authentication is performed as follows:
  - If the MAC address matches an entry in the preconfigured allowed MAC list, the host is allowed.
  - If the MAC address does not match an entry in the preconfigured allowed MAC list, the switch generates a <user name, password> pair, which it forwards to the network RADIUS server for authentication. For more information about the generated credentials, see Non-EAPOL MAC RADIUS authentication on page 101.

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

  EAPOL authentication is not affected.
- For RADIUS-authenticated non-EAPOL hosts, VLAN information from RADIUS is ignored. Upon successful authentication, untagged traffic is put in a VLAN preconfigured for the port.
- For RADIUS-authenticated non-EAPOL hosts, VLAN information from RADIUS is ignored. Upon successful authentication, untagged traffic follows the PVID of the port.
- Non-EAPOL hosts continue to be allowed on the port until the maximum number of non-EAPOL hosts is reached. The maximum number of non-EAPOL hosts allowed is configurable.

- After the maximum number of allowed non-EAPOL hosts is reached, any data packets received from additional non-EAPOL hosts are dropped. The additional non-EAPOL hosts are counted as intruders. New EAPOL hosts can continue to negotiate EAPOL authentication.
- When the intruder count reaches 32, a SNMP trap and system log message are generated. The port administrative status is set to force-unauthorized, and you must reset the port administrative status (from force-unauthorized to auto) to allow new EAPOL and non-EAPOL negotiations on the port.
- The feature uses enterprise-specific MIBs.
- Configuration settings are saved across resets.

Non-EAPOL MAC RADIUS authentication

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

- The user name is the Non-EAPOL MAC address in string format.
- The password is a string that combines the MAC address, switch IP address, unitPort.

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.

Important:

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

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

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

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

Starting with Release 5.0, there is a new rule for Non-EAPOL MAC RADIUS Authentication—when you set the password format to use only the MAC address, the format omits the two dots at the end. Example: password = 010010011253

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

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

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

Multiple Host with Single Authentication

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

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

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

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

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

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

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

MHSA No-Limit

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

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

802.1X Non-EAP client re-authentication

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

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

- Configuring port-based EAPOL using EDM on page 147
- Modifying EAPOL-based security parameters for a specific port using CLI on page 111

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

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

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

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

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

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

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

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

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

Note:

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

NEAP Not Member of VLAN

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

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

Note:

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

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

802.1X or non-EAP with Fail Open VLAN

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

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

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

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

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

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

Important:

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

Important:

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

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

EAPoL Fail Open VLAN on a port

EAPoL Fail Open VLAN provides network connectivity when a switch cannot connect to the RADIUS server. In the MHMV mode, when the switch detects that the RADIUS servers are unreachable, the port is copied to the Fail Open VLAN. In the MHSA mode, the port VLAN Id (PVID) acts as the Fail Open VLAN. All clients already authenticated continue to access the RADIUS-assigned VLAN, while all the new clients access the Fail Open VLAN. This prevents clients from being disconnected when the re-authentication timer expires, by providing them some form of network connectivity.

Note:

When Fail Open VLAN is enabled on a port, port-level configuration always takes precedence over the global settings.

Non-EAP freeform password

When you configure the RADIUS password, you can also use the following commands:

- `show eapol multihost non-eap-pwd-fmt`—this command shows the password fields and padding.

- `show eapol multihost non-eap-pwd-fmt key`—this command prints the key used. The password is printed in cleartext only when password security is not enabled. Otherwise, the password is printed as a string of asterisks.

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 in single allocation mode, since the source MAC is added into the classifier when installing it. As a best practice, use either the best-effort mode (the default mode) or the double allocation mode.

802.1X dynamic authorization extension (RFC 5176)

With 802.1X dynamic authorization extension (RFC 5176), you can enable a third party device to dynamically change VLANs on switches or close user sessions.

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

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

  Important:

  The term RADIUS server, which designates the device that sends the requests, is replaced in RFC 5176 with the term Dynamic Authorization Client (DAC). The NAS is the Dynamic Authorization Server (DAS).
- 802.1X client—the device that requires authentication and uses the switch services.

Important:

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

A switch can receive disconnect or CoA commands in the following conditions:

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

802.1X dynamic authorization extension (RFC 5176) applies only to Extensible Authentication Protocol (EAP) clients and does not affect non-EAP clients.

802.1X dynamic authorization extension supports the following configured features:

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

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

802.1X dynamic authorization extension functions with MHSA port operating mode.

The following authorization considerations apply:

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

To enable the 802.1X dynamic authorization extension feature on the switch, you must perform the following tasks:

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

Important:

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

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

The DAC must use the source IP address of the RADIUS UDP packet to determine which shared secret to accept for RADIUS requests to be forwarded by a proxy. When RADIUS requests are forwarded by a proxy, the NAS-IP-Address attribute will not match the source IP address observed by the DAC. The DAC cannot resolve the NAS-Identifier attribute, whether a proxy is present. The authenticity check performed by the DAC cannot verify the NAS identification attributes, which makes it possible for an unauthorized NAS to forge identification attributes and impersonate an authorized NAS in your network.

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

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

- IEEE 802.1X standard (EAP)
- RFC 2865—RADIUS
- RFC 5176—Dynamic Authorization Extensions to RADIUS

802.1X EAP and NEAP Accounting

Note:

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

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

EAP (802.1X) accounting

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

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

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

Non-EAP accounting

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

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

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

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

NEAP accounting supports the following authentication methods:

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

802.1X EAP Separate enable/disable

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

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

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

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

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

Feature	Behavior
Single-Host	When in Single Host (multihost is disabled) this setting has no effect on the EAP packets – this setting is a multihost specific setting.
Multihost	Only when multihost is enabled per port than this setting will be applied to the port.
Non-EAP	When multihost and non-EAP are enabled per port, then the functionality is presented in the single-host and multi-host.
VLAN assignment for EAP clients	If the user decides to disable or enable EAP protocol on a port, then the VLAN assignment works for the remaining client types (non-EAP); the existing applied settings on a port for authenticated clients are kept.
VLAN assignment for NEAP clients	If you assign the VLAN for an authenticated EAP or NEAP client, then the VLAN is kept if authenticated clients are present on port.
VLAN assignment for EAP or NEAP clients	If you assign the VLAN for an authenticated EAP or NEAP client, then the VLAN is kept if authenticated clients are present on the port, no matter the client types.
Guest-VLAN	There is no restriction to disable the EAP protocol if you enable the Guest VLAN globally and per port (both EAP and non-EAP).

EAPOL-Based Security Configuration using CLI

This section provides procedures to configure network access control on an internal Local Area Network (LAN) with Extensible Authentication Protocol over LAN (EAPOL) using CLI.

Important:

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

Enabling or disabling EAPOL-based security

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To enable EAPOL-based security, enter the following command:

   ```
   eapol enable
   ```

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

   ```
   eapol disable
   ```

Modifying EAPOL-based security parameters for a specific port

Procedure

1. Enter Ethernet Interface Configuration mode:

   ```
   enable

   configure terminal

   interface Ethernet <port>
   ```

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>] [radius-dynamic-server enable] [supplicant-
   timeout <num>] [server-timeout <num>] [max-request <num>]
   ```

Variable definitions

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

Variable	Value
init	Reinitiates EAP authentication.
max-request <num>	Enter the number of times to retry sending packets to supplicant.
port <portllist>	Specifies the ports to configure for EAPOL; enter the port numbers you want to use. **Important:** If you omit this parameter, the system uses the port number that you specified when you issued the **interface** command.
quiet-interval <num>	Enter the number of seconds that you want between an authentication failure and the start of a new authentication attempt; the range is 1 to 65535.
radius-dynamic-server enable	Enables the switch to process requests from the RADIUS Dynamic Authorization server.
re-authentication {enable|disable}	Enables or disables reauthentication.
re-authentication-period <1-604800>	Specifies the number of seconds that you want between re-authentication attempts. Use either this variable or the reauthentication-interval variable; do

Table continues…

Variable	Value
	not use both variables because they control the same setting.
re-authenticate	Specifies an immediate reauthentication.
server-timeout <num>	Specifies a waiting period for response from the server. Enter the number of seconds that you want to wait; the range is 1-65535.
status {authorized|unauthorized|auto}	Specifies the EAP status of the port: • *authorized*— Port is always authorized. • *unauthorized*— Port is always unauthorized. • *auto*— Port authorization status depends on the result of the EAP authentication.
supplicant-timeout <num>	Specifies a waiting period for response from supplicant for all EAP packets, except EAP Request/ Identity packets. Enter the number of seconds that you want to wait; the range is 1-65535.
traffic-control {in-out|in}	Sets the level of traffic control: • *in-out*— If EAP authentication fails, both ingressing and egressing traffic are blocked. • *in*— If EAP authentication fails, only ingressing traffic is blocked.

Setting the guest VLAN for EAPOL

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Disabling guest VLAN for EAPOL

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

   OR

   ```
   default eapol guest-vlan
   ```

Displaying the current EAPOL-based security status

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Example

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

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

Resetting EAP settings globally

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

This command resets the following EAP settings:

- EAP state
- Fail Open VLAN
- VoIP VLANs

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   default eap-all
   ```

Resetting EAP settings at the port level

About this task

This command resets the following settings:

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

Procedure

1. Enter Ethernet Interface Configuration mode:

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

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

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

Displaying EAPOL diagnostics

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Example

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

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

Displaying EAPOL statistics

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Example

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

```
Switch#show eapol auth-stats interface
Port:  1
```

```
    EapolFramesRx:           0
    BackendAuthFails:        0
    EapolFramesTx:           0
    EapolStartFramesRx:      0
    EapolLogoffFramesRx:     0
    EapolRespIdFramesRx:     0
    EapolRespFramesRx:       0
    EapolReqIdFramesTx:      0
    EapolReqFramesTx:        0
    InvalidEapolFramesRx:    0
    EapLengthErrorFramesRx:  0
    LastEapolFrameVersion:   0
    LastEapolFrameSource:    0000:0000:0000
Port:  2
    EapolFramesRx:           0
    BackendAuthFails:        0
    EapolFramesTx:           0
    EapolStartFramesRx:      0
    EapolLogoffFramesRx:     0
    EapolRespIdFramesRx:     0
    EapolRespFramesRx:       0
----More (q=Quit, space/return=Continue)----
```

Displaying EAPOL guest VLAN settings

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

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

   ```
   show eapol guest-vlan
   ```

Example

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

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

Configuring global EAPOL multihost settings

Use the following procedure to control the global multihost settings.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

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

```
eapol multihost { [adac-non-eap-enable] [allow-non-eap-enable]
[auto-non-eap-mhsa-enable] [block-different-radius-assigned-vlan]
[eap-packet-mode] [eap-protocol-enable] [non-eap-phone-enable] [non-
eap-reauthentication-enable] [non-eap-use-radius-assigned-vlan]
[radius-non-eap-enable] [use-most-recent-radius-vlan] [use-radius-
assigned-vlan] [multivlan enable] [non-eap-pwd-fmt {[ip-addr] [mac-
addr]] [port-number]}]}
```

Variable definitions

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

Variable	Value
adac-non-eap-enable	Allows authentication of non-EAP Phones using ADAC.
allow-non-eap-enable	Enables MAC addresses of non-EAP clients.
auto-non-eap-mhsa-enable	Enables auto-authentication of non-EAP clients in MHSA mode.
block-different-radius-assigned-vlan	Blocks subsequent MAC authentications if the RADIUS assigned VLAN is different than the first authorized station VLAN.
eap-packet-mode	Selects the packet mode for EAP authentication. Values are: • multicast • unicast
eap-protocol-enable	Enables EAP protocol on ports.
non-eap-phone-enable	Enables the use of non-EAP IP phone clients.
non-eap-reauthentication-enable	Enables re-authentication for NEAP clients.
non-eap-use-radius-assigned-vlan	Enables the use of VLAN IDs assigned by RADIUS for non-EAP clients.
radius-non-eap-enable	Enables RADIUS authentication of non-EAP clients.
use-most-recent-radius-vlan	Allows the use of the most recently assigned RADIUS VLAN.
use-radius-assigned-vlan	Allows the use of RADIUS-assigned VLAN IDs.
non-eap-pwd-fmt *{[ip-addr][mac-addr][port-number]}*	Sets bits in RADIUS non-EAPOL password format.

Disabling global EAPOL multihost settings

Use the following procedure to disable EAPOL multihqost settings.

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

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

```
no eapol multihost { [adac-non-eap-enable] [allow-non-eap-enable]
[auto-non-eap-mhsa-enable] [block-different-radius-assigned-vlan]
[eap-protocol-enable] [non-eap-phone-enable] [non-eap-
reauthentication-enable] [non-eap-use-radius-assigned-vlan] [radius-
non-eap-enable] [use-most-recent-radius-vlan] [use-radius-assigned-
vlan] [multivlan enable] [non-eap-pwd-fmt {[ip-addr] [mac-addr]]
[port-number]}]}
```

Variable definitions

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

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

Restoring global EAPOL multihost settings to default

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

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

   ```
   default eapol multihost { [adac-non-eap-enable] [allow-non-eap-
   enable] [auto-non-eap-mhsa-enable] [block-different-radius-assigned-
   vlan] [eap-packet-mode] [eap-protocol-enable] [non-eap-phone-enable]
   [non-eap-reauthentication-enable] [non-eap-use-radius-assigned-vlan]
   [radius-non-eap-enable] [use-most-recent-radius-vlan] [use-radius-
   assigned-vlan] [multivlan enable] [non-eap-pwd-fmt {[ip-addr] [mac-
   addr]] [port-number]}]}
   ```

Variable definitions

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

Variable	Value
adac-non-eap-enable	Resets authentication of non-EAP Phones using ADAC.
allow-non-eap-enable	Resets control of MAC addresses of non-EAP clients.
auto-non-eap-mhsa-enable	Disables auto-authentication of non-EAP clients in MHSA mode.
block-different-radius-assigned-vlan	Disables the blocking of subsequent MAC authentications if the RADIUS assigned VLAN is different than the first authorized station VLAN.
eap-packet-mode	Defaults the type of packet used for initial EAP request for IDs (multicast).
eap-protocol-enable	Resets EAP protocol to enabled (default).
non-eap-phone-enable	Disables the use of non-EAP IP phone clients
non-eap-reauthentication-enable	Disables re-authentication for non-EAP clients.
non-eap-use-radius-assigned-vlan	Disables the use of VLAN IDs assigned by RADIUS for non-EAP clients
radius-non-eap-enable	Disables RADIUS authentication of non-EAP clients.
use-most-recent-radius-vlan	Disables the use of the most recent RADIUS-assigned VLAN.
use-radius-assigned-vlan	Disables the use of RADIUS-assigned VLAN IDs.
multivlan enable	Disables multiple VLAN capabilities for EAP and non-EAP hosts.
non-eap-pwd-fmt *{[ip-addr][mac-addr][port-number]}*	Restores default format for RADIUS non-EAPOL password attribute.

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

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

Procedure

1. Enter Ethernet Interface Configuration mode:

   ```
   enable

   configure terminal

   interface Ethernet <port>
   ```

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

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

Variable definitions

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

Variable	Value
adac-non-eap-enable	Enables authentication of non-EAP Phones using ADAC.
allow-non-eap-enable	Enables MAC addresses of non-EAP clients.
auto-non-eap-mhsa-enable	Enables auto-authentication of non-EAP clients in MHSA mode.
block-different-radius-assigned-vlan	Blocks subsequent MAC authentication if the RADIUS-assigned VLAN is different from the first authorized station VLAN.
eap-mac-max <1–32>	Specifies the maximum number of EAP-authenticated MAC addresses allowed.
eap-packet-mode <multicast | unicast>	Specifies the type of packet used for initial EAP request for IDs.
eap-protocol-enable	Enables EAP protocol on the port.
enable	Allows EAP clients (MAC addresses).

Table continues…

Variable	Value
mac-max <1–64>	Specifies the maximum number of MAC addresses allowed per port.
mhsa-no-limit	Allows an unlimited number of auto-authenticated non-EAP clients on the port.
non-eap-mac-max <1–32>	Specifies the maximum number of non-EAP authenticated MAC addresses allowed.
non-eap-phone-enable	Allows the use of non-EAP IP phone clients.
non-eap-use-radius-assigned-vlan	Allows the use of RADIUS assigned VLAN IDs for non-EAP clients.
port <portlist>	Specifies the port number or list of ports on which to apply EAPOL multihost settings.
radius-non-eap-enable	Enables RADIUS authentication of non-EAP clients.
use-most-recent-radius-vlan	Enables use of the most recent RADIUS-assigned VLAN.
use-radius-assigned-vlan	Allows the use of RADIUS-assigned VLAN value.
non-eap-mac [port <portlist>] {H.H.H }	Allows a non-EAPOL MAC address.

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

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

Procedure

1. Enter Ethernet Interface Configuration mode:

   ```
   enable

   configure terminal

   interface Ethernet <port>
   ```

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

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

Variable definitions

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

Variable	Value
adac-non-eap-enable	Disables authentication of non-EAP Phones using ADAC.
allow-non-eap-enable	Disables MAC addresses of non-EAP clients
auto-non-eap-mhsa-enable	Disables auto-authentication of non-EAP clients in MHSA mode.
block-different-radius-assigned-vlan	Disables the blocking of subsequent MAC authentication if the RADIUS-assigned VLAN is different from the first authorized station VLAN.
eap-protocol-enable	Disables EAP protocol on the port.
enable	Disallows EAP clients (MAC addresses).
mhsa-no-limit	Limits the number of auto-authenticated non-EAP clients.
non-eap-phone-enable	Disables the use of non-EAP IP phone clients.
non-eap-use-radius-assigned-vlan	Disables the use of RADIUS assigned VLAN IDs for non-EAP clients.
port <portlist>	Specifies the port number or list of ports on which to apply EAPOL multihost settings.
radius-non-eap-enable	Disables RADIUS authentication of non-EAP clients.
use-most-recent-radius-vlan	Disables the use of the most recent RADIUS-assigned VLAN.
use-radius-assigned-vlan	Disallows the use of RADIUS-assigned VLAN value.
non-eap-mac [port <portlist>] {delete-all | H.H.H}	Disallows a non-EAPOL MAC address or deletes all local non-EAP clients.

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

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

Procedure

1. Enter Ethernet Interface Configuration mode:

   ```
   enable

   configure terminal

   interface Ethernet <port>
   ```

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

   ```
   default eapol multihost [adac-non-eap-enable] [allow-non-eap-enable]
   [auto-non-eap-mhsa-enable] [block-different-radius-assigned-vlan]
   ```

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

Variable definitions

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

Variable	Value
adac-non-eap-enable	Resets authentication of non-EAP Phones using ADAC.
allow-non-eap-enable	Resets control of non-EAP clients (MAC addresses) to default (disabled).
auto-non-eap-mhsa-enable	Disables auto-authentication of non-EAP clients.
block-different-radius-assigned-vlan	Disables the blocking of subsequent MAC authentication if the RADIUS-assigned VLAN is different from the first authorized station VLAN.
eap-mac-max	Resets the maximum number of EAP-authenticated MAC addresses allowed to default (1).
eap-packet-mode	Resets the EAP packet mode to the default (multicast).
eap-protocol-enable	Enables EAP protocol on the port.
enable	Resets control of whether EAP clients (MAC addresses) are allowed to default (disabled).
mac-max	Resets the maximum number of clients allowed on the port to the default value (1).
mhsa-no-limit	Limits the number of auto-authenticated non-EAP clients.
non-eap-mac-max	Resets maximum number of non-EAP authenticated MAC addresses allowed to default.
non-eap-phone-enable	Disables the use of non-EAP IP phone clients.
non-eap-use-radius-assigned-vlan	Disables the use of RADIUS assigned VLAN IDs for non-EAP clients.
port <portlist>	Specifies the port number or list of ports on which to default the EAPOL multihost configuration.
radius-non-eap-enable	Resets RADIUS authentication of non-EAP clients to default.
use-most-recent-radius-vlan	Disables the use of the most recent RADIUS-assigned VLAN.
use-radius-assigned-vlan	Disallows the use of RADIUS-assigned VLAN value.
non-eap-mac [port <portlist>] {default-all | H.H.H}	Resets the non-EAPOL MAC addresses to default.

Setting the maximum number of clients allowed per port

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

You can use the **eapol multihost mac-max** command with **eap-mac-max** and **non-eap-mac-max** commands. The value set by **mac-max** takes precedence over other commands. Even if you set **eap-mac-max** or **non-eap-mac-max** to a higher limit, the limit set using the **mac-max** command cannot be exceeded.

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

The syntax for the eapol multihost mac-max command is

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

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

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

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

Note:

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

Example 1::

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

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

Example 2::

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

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

Example 3::

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

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

Example 4::

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

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

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

Procedure

1. Enter VLAN Interface Configuration mode:

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

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

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

Variable definitions

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

Variable	Value
port <portlist>	Specify the port or ports on which to apply EAPOL settings.
<H.H.H>	Specifies the MAC address of the allowed non-EAPOL host.

Displaying global settings for non-EAPOL hosts on EAPOL-enabled ports

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show eapol multihost
   ```

Example

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

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

Variable definitions

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

Variable	Value
interface	Displays EAPOL multihost port configuration.
non-eap-mac	Displays allowed non-EAPOL MAC address.
status	Displays EAPOL multihost port status.

Displaying non-EAPOL support settings for each port

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Example

The following figure provides a sample of **show eapol multihost interface** [<portList>].

```
Switch#show eapol multihost interface
Unit/Port:  1/1
    MultiHost Status                                 :  Disabled
    Total Maximum Nuber of Clients                   :  2
    Maximum Number of EAP Clients                    :  1
    Maximum Number of Non-EAP Clients                :  1
    Allow Local Non-EAP Clients                      :  Disabled
    Non-EAP RADIUS Authentication                    :  Disabled
    Non-EAP AutoLearned After Single Auth (MHSA)     :  Disabled
    Non-EAP DHCP Phone Authentication                :  Disabled
```

```
    EAPoL Request Packet Generation Mode                :  Multicast
    EAP RADIUS Assigned VLANs                           :  Disabled
    Non-EAP RADIUS Assigned VLANs                       :  Disabled
    EAP Protocol                                        :  Enabled
    Use Most Recent RADIUS Assigned VLAN                :  Disabled
    Block Different RADIUS Assigned VLAN Authentication :  Disabled
    ADAC Non-EAP Phone Authentication                   :  Disabled
    MHSA No limit Non-EAP Authentication                :  Disabled
...
```

Displaying non-EAPOL hosts information

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show eapol multihost non-eap-mac status [<portList>]
   ```

Example

The following figure provides a sample of **show eapol multihost non-eap-mac status**.

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

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

Use the following procedures to configure non-EAPOL authentication.

To configure support for non-EAPOL hosts on EAPOL-enabled ports, perform the following:

1. Enable non-EAPOL support globaly on the switch and locally (for the desired interface ports), using one or both of the following authentication methods:
   a. local authentication
   b. RADIUS authentication
2. Enable EAPOL multihost on ports.
3. Specify the maximum number of non-EAPOL MAC addresses allowed on a port.
4. For local authentication only, identify the MAC addresses of non-EAPOL hosts allowed on the ports.

By default, support for non-EAPOL hosts on EAPOL-enabled ports is disabled.

Enabling local authentication of non-EAPOL hosts on EAPOL-enabled ports

For local authentication of non-EAPOL hosts on EAPOL-enabled ports, you must enable the feature globally on the switch and locally for ports on the interface.

Procedure

1. To enable local authentication of non-EAPOL hosts globally on the switch, perform the following:
   a. Log on to CLI in Global Configuration command mode.
   b. At the command prompt, enter the following command:

   ```
   eapol multihost allow-non-eap-enable
   ```

2. To enable local authentication of non-EAPOL hosts for a specific port or for all ports on an interface, perform the following:
   a. Log on to CLI in Interface Configuration command mode.
   b. At the command prompt, enter the following command:

   ```
   eapol multihost [port <portlist>] allow-non-eap-enable
   ```

Variable definitions

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

Variable	Value
port <portlist>	Specifies the port or list of ports on which you want to enable non-EAPOL hosts using local authentication. If you do not specify a port parameter, the command applies to all ports on the interface.

Enabling RADIUS authentication of non-EAPOL hosts on EAPOL-enabled ports

For RADIUS authentication of non-EAPOL hosts on EAPOL-enabled ports, you must enable the feature globally on the switch and locally for ports on the interface.

Procedure

1. To enable RADIUS authentication of non-EAPOL hosts globally on the switch, perform the following:.
   a. Log on to CLI in Global Configuration command mode.
   b. At the command prompt, enter the following command:

   ```
   eapol multihost radius-non-eap-enable
   ```

2. To enable RADIUS authentication of non-EAPOL hosts for a specific port or for all ports on an interface, perform the following:
   a. Log on to CLI in Interface Configuration command mode.
   b. At the command prompt, enter the following command:

```
eapol multihost [port <portlist>] radius-non-eap-enable
```

Variable definitions

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

Variable	Value
port <portlist>	Specifies the port or ports on which you want RADIUS authentication enabled. If you do not specify a port parameter, the command applies to all ports on the interface.

Configure 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.

Table continues…

Parameter	Description
no-padding	The RADIUS password uses dots only to separate fields. This is the default setting.

Set 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.

Display 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:**********
```

Viewing the non-EAP client re-authentication status

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

Procedure

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

```
show eapol multihost
```

Example

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

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

Clearing non-EAP authenticated clients from ports

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

Procedure

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

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

Variable definitions

The following table describes the parameters for the **clear eapol non-eap** command.

Variable	Value
<portlist>	Specifies a port or ports from which to clear authenticated NEAP clients. If you do not specify a port parameter, the command applies to all ports.
address <H.H.H>	Specifies the MAC address of an authenticated NEAP client to clear from the port. If you enter a MAC address value of 00:00:00:00:00:00, all authenticated NEAP clients are cleared from the specified port.

Configuring the maximum number of non-EAPOL hosts allowed

Use the following procedure to configure the maximum number of non-EAPOL hosts allowed for a specific port or for all ports on an interface.

Procedure

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

```
eapol multihost [port <portlist>] non-eap-mac-max <1–32>
```

Variable definitions

The following table describes the parameters for the **eapol multihost non-eap-mac-max**command.

Variable	Value
port <portlist>	Specifies the port or ports to which you want the setting to apply. If you do not specify a port parameter, the command sets the value for all ports on the interface.
<1–32>	Specifies the maximum number of non-EAPOL clients allowed on the port at any one time. The default is 1.

Important:

The configurable maximum number of non-EAPOL clients for each port is 32, however Extreme Networks expects that the usual maximum allowed for each port be lower. Extreme Networks expects that the combined maximum will be approximately 200 per switch.

Creating the allowed non-EAPOL MAC address list

Use the following procedure to specify the MAC addresses of non-EAPOL hosts allowed on a specific port or on all ports on an interface for local authentication.

Procedure

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

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

Variable definitions

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

Variable	Value
port <portlist>	Specifies the port or ports on which you want to allow the specified non-EAPOL hosts. If you do not specify a port parameter, the command applies to all ports on the interface.
<H.H.H>	Specifies the MAC address of the allowed non-EAPOL host.

Enabling or disabling Non-EAP client re-authentication

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

Procedure

1. Log on to CLI in Global Configuration command mode.
2. To enable non-EAP re-authentication, enter the following command:

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

3. To disable non-EAP re-authentication, enter the following command:

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

   OR

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

Configuring 802.1X dynamic authorization extension (RFC 5176) configuration using CLI

Configuring RADIUS dynamic authorization extension (802.1X RFC 5176)

Use the following procedure to configure RADIUS dynamic authorization extension (802.1X RFC 5176) to enable and configure RADIUS dynamic authorization extension parameters on the switch.

Before you begin

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

Important:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Disabling RADIUS dynamic authorization extension (802.1X RFC 5176)

Use the following procedure to disable RADIUS dynamic authorization extension (802.1X RFC 5176) to prevent the RADIUS server from sending a change of authorization (CoA) or disconnect command to the Network Access Server (NAS).

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Viewing RADIUS dynamic authorization client configuration

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Variable definitions

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

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

Viewing RADIUS dynamic authorization client statistics

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Variable definitions

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

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

Enabling or disabling RADIUS dynamic authorization extension (802.1X RFC 5176) on a port

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

Before you begin

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

Important:

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

Procedure

1. Enter Ethernet Interface Configuration mode:

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

2. To enable RADIUS dynamic authorization extension on a port, enter the following command:

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

   OR

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

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

Viewing replay protection for RADIUS dynamic authorization extension

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

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

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

Enabling or disabling replay protection for RADIUS dynamic authorization extension

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

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. To enable or re-enable replay protection, enter the following command:

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

OR

To disable replay protection, enter the following command:

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

Configuring 802.1X or Non-EAP and Guest VLAN on the same port using CLI

Use the following sections to allow 802.1X or Non-EAP devices to function with Guest VLAN enabled on the same port.

Enabling EAPOL VoIP VLAN

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Variable definitions

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

Variable	Value
enable	Enables the VoIP VLAN.
<1–5>	Specifies the number of VoIP VLAN. RANGE: 1 to 5
vid *<1–4094>*	Specifies the VLAN ID. RANGE: 1 to 4094

Disabling EAPOL VoIP VLAN

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

Variable	Value
enable	Disables the VoIP VLAN.
<1–5>	Specifies the number of VoIP VLAN, range of 1 to 5.

Configuring EAPOL VoIP VLAN as the default VLAN

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

The following table describes the parameters for the **`default eapol mulihost voip-vlan`** command.

Variable	Value
enable	Enables the VoIP VLAN.
<1–5>	Specify the number of VoIP VLAN, range of 1 to 5.
vid	Default VoIP VLAN ID.

Viewing EAPOL VoIP VLAN

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Configuring EAPoL Fail Open VLAN using CLI

Use the following sections to configure Extensible Authentication Protocol over LAN (EAPoL) Fail Open VLAN using the CLI.

Configure EAPoL Fail Open VLAN

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command:

   ```
   eapol multihost fail-open-vlan {[enable] | [vid <1-4094>] |
   [continuity-mode <enable>]}
   ```

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 globally.
vid *<1–4094>*	Specifies the Fail Open VLAN ID. Range: 1 to 4094

Enable EAPoL Fail Open VLAN Continuity Mode

About this task

Use this procedure to enable the EAPoL Fail Open VLAN continuity mode.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Enable EAPoL Fail Open VLAN continuity mode:

```
eapol multiHost fail-open-vlan continuity-mode enable
```

Disable EAPoL Fail Open VLAN Continuity mode

About this task

Use this procedure to disable EAPoL Fail Open VLAN continuity mode.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Disable EAPoL Fail Open VLAN continuity mode:

```
no eapol multihost fail-open-vlan continuity-mode enable
```

Enable EAPoL Fail Open VLAN on a Port

Before you begin

Ensure that the port is associated with a VLAN, which can either be the global VLAN or a configured VLAN other than the global VLAN.

Procedure

1. Enter Ethernet Interface Configuration mode:

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

2. Enable Fail Open VLAN on a single port or multiple ports:

```
eapol multihost fail-open-vlan port <portlist> enable vid <1-4059>
```

Note:

If Fail Open VLAN is enabled on a port, port-level configuration always takes precedence over the global settings.

Important:

Ensure that you use a static VLAN Id when you enable the Fail Open VLAN. Fail Open VLAN does not work after a reboot if you create a dynamic VLAN.

3. Verify the configuration:

```
show eapol multihost fail-open-vlan interface <portlist>
```

Example

The following example configures and verifies the configuration of Fail Open VLAN on port 15.

Create the port-based VLAN:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#vlan create 100 type port
```

Enable Fail Open VLAN on port 15:

```
Switch:1(config)#interface ethernet 15
Switch:1(config-if)#eapol multihost fail-open-vlan port 15 enable vid 100
```

View VLAN settings and port membership:

```
Switch:1#show vlan interface verbose 15

     Filter Filter
     Untag. Unreg.
Port Frames Frames PVID VLAN VLAN Name         PRI Tagging       Port Name
---- ------ ------ ---- ---- ---------------- --- ------------- --------------
15    No     Yes    1    100  VLAN #100        0   UntagAll      Port 15
---- ------ ------ ---- ---- ---------------- --- ------------- --------------
```

Verify Fail Open VLAN configuration on port 15:

```
Switch:1#show eapol multihost fail-open-vlan interface 15

     Fail-Open Fail-Open    Fail-Open
Port   Vlan     Vlan ID       UBP
---- -------- ---------- ----------------
15    Enabled     100      N/A
```

Variable Definitions

Use the data in the following table to use the **`eapol multihost fail-open-vlan`** command.

Variable	Value
port *<portlist>*	Specifies a single port or multiple ports on which to enable Fail Open VLAN. Separate multiple ports with a comma.
vid *<1-4059>*	Specifies the Fail Open VLAN Id.

Enable EAPoL Fail Open VLAN on a Port Assigned to a PVID

About this task

Use this procedure to enable Fail Open VLAN on a port assigned to a port VLAN ID (PVID). In this case, the port PVID acts as the Fail Open VLAN when the RADIUS server is unreachable.

Note:

Port-level Fail Open VLAN configuration always takes precedence over global configuration.

Procedure

1. Enter Ethernet Interface Configuration mode:

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

2. Enable EAPoL Fail Open VLAN on a port assigned to a PVID:

```
eapol multihost fail-open-vlan port <portlist> enable vid port-pvid
```

3. Verify the configuration:

```
show eapol multihost fail-open-vlan interface <portlist>
```

Example

The following example configures and verifies the configuration of Fail Open VLAN on a port assigned to a PVID.

Verify port 16 is associated with a port VLAN Id (PVID):

```
Switch:1(config)#interface ethernet 16
Switch:1(config-if)#show eapol multihost fail-open-vlan interface 16

     Fail-Open Fail-Open    Fail-Open
Port   Vlan     Vlan ID       UBP
---- -------- ---------- ----------------
16    Disabled  Port-PVID     N/A
```

Enable EAPoL Fail Open VLAN on port 16:

```
Switch:1(config-if)#eapol multihost fail-open-vlan port 16 enable vid port-pvid
```

Verify the configuration:

```
Switch:1#show eapol multihost fail-open-vlan interface 16

     Fail-Open Fail-Open    Fail-Open
Port   Vlan     Vlan ID       UBP
---- -------- ---------- ----------------
16    Enabled   Port-PVID     N/A
```

Variable Definitions

Use the data in the following table to use the **`eapol multihost fail-open-vlan`** command.

Variable	Value
port *<portlist>*	Specifies a single port or multiple ports on which to enable Fail Open VLAN. Separate multiple ports with a comma.
vid *<1-4059>*	Specifies the Fail Open VLAN Id.

Display Global EAPoL Fail Open VLAN settings

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display global Fail Open VLAN settings:

   ```
   show eapol multihost fail-open-vlan
   ```

Display EAPoL Fail Open VLAN on a Port or Port Assigned to a PVID

About this task

Use this procedure to view Fail Open VLAN settings on a port or a port assigned to a PVID.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View Fail Open VLAN configuration:

   ```
   show eapol multihost fail-open-vlan interface <portlist>
   ```

Example

The following is an example of `show eapol multihost fail-open-vlan` on a port or port assigned to a PVID:

```
Switch:1#show eapol multihost fail-open-vlan interface 15,16

     Fail-Open Fail-Open    Fail-Open
Port   Vlan     Vlan ID       UBP
---- -------- ---------- ----------------
15    Enabled    100          N/A
16    Enabled    Port-PVID    N/A
```

Variable Definitions

Use the data in the following table to use the **`eapol multihost fail-open-vlan`** command.

Variable	Value
port *<portlist>*	Specifies a single port or multiple ports on which to enable Fail Open VLAN. Separate multiple ports with a comma.
vid *port-pvid*	Specifies the port VLAN Id (PVID) that acts as the Fail Open VLAN.

Display EAPoL Fail Open VLAN Continuity mode

About this task

Use 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 continuity mode:

   ```
   show eapol multihost fail-open-vlan
   ```

   OR

   ```
   show eapol multihost
   ```

Configuring 802.1X or non-EAP Last Assigned RADIUS VLAN

Configuring use of the most recent RADIUS VLAN

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   [no] [default] eap multihost use-most-recent-radius-vlan
   ```

Restoring use of the most recent RADIUS VLAN to default

Use the following procedure to restore the use most recent RADIUS assigned VLAN status to default.

Procedure

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

   ```
   default eap multihost use-most-recent-radius-vlan
   ```

Displaying EAPOL multihost status

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show eapol multihost
   ```

Example

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

```
Switch#show eapol multihost
Allow Non-EAPOL Clients:  Disabled
Use RADIUS To Authenticate Non-EAPOL Clients:  Disabled
```

```
Allow Non-EAPOL Clients After Single Auth (MHSA):  Disabled
Allow Non-EAPOL VoIP Phone Clients:  Disabled
EAPOL Request Packet Generation Mode:  Multicast
Allow Use of RADIUS Assigned VLANs:  Disabled
Allow Use of Non-Eapol RADIUS Assigned VLANs:  Disabled
Non-EAPOL RADIUS Password Attribute Format:  IpAddr.MACAddr.PortNumber
Use most recent RADIUS VLAN:  Disabled
Non-EAP re-authentication:  Disabled
```

Configuring EAPOL using EDM

This section provides procedures to 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 features, such as UDP Forwarding and IP Source Guard, that use QoS policies.

Configure EAPoL Globally using EDM

Use the following procedure to configure EAPoL globally to configure EAPoL parameters for the switch.

Procedure

1. In the navigation pane, expand the **Security** folder.
2. Double-click **802.1X/EAP**.
3. On the **EAPOL** tab, configure the EAPoL parameters as required.
4. On the toolbar, click **Apply**.

Field Descriptions

Use the data in the following table to configure EAPoL globally.

Field	Description
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.
GuestVlanEnabled	Enables or disables the Guest VLAN.
GuestVlanId	Sets the VLAN ID of the Guest VLAN.

Table continues…

Field	Description
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.
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.
MultiHostUseMostRecentRadiusAssignedVlan	Enables or disables the use of the most recent RADIUS VLAN. **Note:** To enable the feature, you must also enable MultiHostUseMostRecentRadiusAssignedVlan on each port.
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. **Important:** The switch does not validate that the 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 that 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	Specifies 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

Table continues…

Field	Description
	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.
AutoPortConfigModeSwitchToMHMV	Specifies the ports for MHMV automatic configuration.
AutoPortConfigModeSwitchToMHMVAction	Applies MHMV automatic configuration on the specified ports.
AutoPortConfigModeSwitchToMHMVStatus	Displays the MHMV automatic configuration status.

Enabling or disabling non-EAP client re-authentication using EDM

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

Procedure

1. In the navigation tree, double-click **Security**.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **EAPOL** tab.
4. Perform one of the following:
   - Select the **MultiHostNeapReauthenticationEnabled** checkbox to enable NEAP re-authentication.
   - Clear the **MultiHostNeapReauthenticationEnabled** checkbox to disable NEAP re-authentication.
5. On the toolbar, click **Apply**.

Configuring port-based EAPOL using EDM

Use this procedure to configure EAPOL security parameters for an individual port or multiple ports.

Procedure

1. In the navigation tree, double-click **Security** to open the security tree.

2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **EAPOL Ports** tab.
4. In a port row, double-click a cell under the column heading for the parameter you want to change.
5. Select a parameter or value from the drop-down list.
6. Repeat the previous two steps to configure other parameters.
7. On the toolbar, click **Apply**.

EAPOL Ports Tab Field Descriptions

Use the data in the following table to use the **EAPOL Ports** tab.

Name	Description
PortNumber	Indicates the port number.
PortInitialize	Enables and disables EAPOL authentication for the specified port.
PortReauthenticateNow	Enables (true) EAPOL authentication for the specified port immediately, without waiting for the Re-Authentication Period to expire.
PaeState	Indicates the EAPOL authorization status for the switch:
BackendAuthState	Indicates the current state of the Backend Authentication state for the switch.
AdminControlledDirections	Indicates the current EAPOL authentication for the port: • **both**: Incoming and outgoing traffic • **in**: Incoming traffic only For example, if you set the specified port field value to both, and EAPOL authentication fails, then both incoming and outgoing traffic on the specified port is blocked.
OperControlledDirections	Indicates the current operational value for the traffic control direction for the port (see the preceding field description).
AuthControlledPortStatus	Indicates the current EAPOL authorization status for the port: • **authorized** • **unauthorized**

Table continues…

Name	Description
AuthControlledPortControl	Indicates the EAPOL authorization status for the port: • **Force Authorized**: The authorization status is always authorized • **Force Unauthorized**: The authorization status is always unauthorized • **Auto**: The authorization status depends on the EAP authentication
QuietPeriod	Indicates the current value of the time interval between any single EAPOL authentication failure and the start of a new EAPOL authentication attempt.
SupplicantTimeout	Indicates the time to wait for response from supplicant for all EAP packets, except EAP Request/ Identity.
ServerTimeout	Indicates the time to wait for a response from the RADIUS server for all EAP packets.
MaximumRequests	Indicates the number of times the switch attempts to resend EAP packets to a supplicant.
ReAuthenticationPeriod	Indicates the time interval between successive reauthentications. When the ReAuthenticationEnabled field (see the following field) is enabled, you can specify the time period between successive EAPOL authentications for the specified port.
ReAuthenticationEnabled	Indicates if reauthentication is enabled. When enabled, the switch performs a reauthentication of the existing supplicants at the time interval specified in the ReAuthenticationPeriod field (see preceding field description).
KeyTxEnabled	Indicates the value of the KeyTransmissionEnabled constant currently in use by the Authenticator PAE state of the switch. This always returns false as key transmission is irrelevant.
LastEapolFrameVersion	Indicates the protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	Indicates the source MAC address carried in the most recently received EAPOL frame.

Configuring advanced port-based EAPoL using EDM

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 Ports** 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 Ports** 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**.

EAPOL Advance Ports Tab Field Descriptions

Use the data in the following table to use the **EAPOL Advance Ports** tab.

Name	Description
PortNumber	Specifies the port number.
DefaultEapAll	Enables or disables the default EAP settings.
GuestVlanEnabled	Enables and disables Guest VLAN on the port.
GuestVlanId	Specifies the ID of a Guest VLAN that the port is able to access while unauthorized. This value overrides the Guest VLAN ID value set for the switch in the EAPOL tab. Specifies zero when switch global guest VLAN ID is used for this port.
MultiHostMaxMacs	Specifies the maximum number of clients allowed on this port. The maximum number ranges between 1 and 64.
MultiHostEapMaxNumMacs	Specifies the maximum number of allowed EAP clients on the port.
MultiHostAllowNonEapClient (MAC addresses)	Enables or disables support for non EAPOL clients using local authentication.
MultiHostNonEapMaxNumMacs	Specifies the maximum number of non EAPOL clients allowed on this port. The default is 1. The maximum number is 32.
MultiHostSingleAuthEnabled	Enables or disables Multiple Host with Single Authentication (MHSA) support for non EAPOL clients.
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…

Name	Description
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.
FailOpenVlanUBP	Specifies the name of the Fail Open VLAN User Based Policy (UBP). Enter an alphanumeric string between 0 and 16 characters.
ProcessRadiusRequestsServerPackets (RADIUS Dynamic Authorization Server)	Enables or disables the processing of RADIUS requests-server packets that are received on this port.
MultiHostClearNeap	Clears a specific, or all authenticated, NEAP clients from the port. To clear a specific client on a port, enter the MAC address of the client. To clear all clients on a port, enter 00:00:00:00:00:00.
MultiHostAdacNonEapEnabled	Enables or disables the non-EAP multihost ADAC settings.

View 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.

Configuring multihost EAP VoIP VLAN using EDM

Use this procedure to activate the multihost VoIP VLAN. You can allow 802.1X or Non-EAP devices to function with the Guest VLAN enabled on the same port.

Procedure

1. In the navigation tree, double-click **Security** to open the security tree.
2. In the security tree, click **802.1X/EAP**.
3. In the work area, click the **EAP VoIP VLAN** tab.
4. In the table, double-click the cell under the column you want to edit.
5. Select a parameter or value form the drop-down list
6. Repeat steps 4 and 5 to configure other parameters.
7. On the toolbar, click **Apply**.

EAP VoIP Vlan Tab Field Descriptions

Use the data in the following table to use the **EAP VoIP VLAN** tab.

Name	Description
MultiHostVoipVlanIndex	Indicates the multihost VoIP VLAN index, range of 1 to 5.
MultiHostVoipVlanEnabled	Enables (true) or disables (false) the multihost VoIP VLAN.
MultiHostVoipVlanId	Indicates the VLAN ID, range of 1 to 4094.

Clearing Non-EAP authenticated clients from ports using EDM

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

Procedure

1. In the navigation tree, double-click **Security** .
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **EAPOL Advance Ports** tab.
4. Click a port row to select a port.
5. Double-click the cell under the **MultiHostClearNeap** column heading.
6. Perform one of the following:
   - To clear a specific authenticated NEAP client from the specified port, type the MAC address of that client in the box.

- To clear all authenticated NEAP clients from the specified port, type a MAC address of 00:00:00:00:00:00 in the box.

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

Viewing Multihost status information using EDM

Use this procedure to display multiple host status for a port.

Procedure

1. From the **Device Physical View**, right-click a port.
2. From the menu, click **Edit**.
3. In the work area, click the **EAPOL Advance** tab.
4. On the tool bar, click **Multi Hosts**.
5. Click the **Multi Host Status** tab.

Multi Host Status Tab Field Descriptions

Use the data in the following table to use the **Multi Host Status** tab.

Name	Description
PortNumber	The port number in use.
ClientMACAddr	The MAC address of the client.
PaeState	The current state of the authenticator PAE state machine.
BackendAuthState	The current state of the Backend Authentication state machine.
Reauthenticate	The current reauthentication state of the machine. When the reauthenticate attribute is set to True, the client reauthenticates.

Viewing Multihost session information using EDM

Use this procedure to view Multihost session information for a port.

Procedure

1. From the **Device Physical View**, right-click a port.
2. From the menu, click **Edit** .
3. In the work area, click the **EAPOL Advance** tab.
4. On the tool bar, click the **Multi Hosts** button.
5. Click the **Multi Host Session** tab.

Multi Host Session Tab Field Descriptions

Use the data in the following table to use the **Multi Host Session** tab.

Name	Description
PortNumber	The port number in use.
ClientMACAddr	The MAC address of the client.
UserName	The user name representing the identity of the supplicant PAE.

Viewing Multihost DHCP authenticated information

Use this procedure to display mutiple host DHCP authenticated information for a port.

Procedure

1. From the **Device Physical View**, right-click a port.
2. From the menu, click **Edit** .
3. In the work area, click the **EAPOL Advance** tab.
4. On the tool bar, click the **Multi Hosts** button.
5. Click the **Multi Host DHCP Authenticated** tab.

Multi Host DHCP Authenticated Tab Field Descriptions

Use the data in the following table to use the **Multi Host DHCP Authenticated** tab.

Name	Description
PortNumber	Specifies the port number.
ClientMACAddr	Specifies the MAC address of the client.
UserName	Specifies the user name representing the identity of the supplicant PAE.

Configuring RADIUS globally using EDM

Use this procedure to configure RADIUS security for the switch.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, double-click **RADIUS**.
3. In the work area, click the **Globals** tab.

4. Perform one of the following:
   - In the RADIUS section, select the **UseMgmtIp** checkbox, to enable RADIUS request use management.
   - In the RADIUS section, clear the **UseMgmtIp** checkbox, to disable RADIUS request use management.
5. Perform one of the following:
   - In the RADIUS section, select the **PasswordFallbackEnabled** checkbox, to enable RADIUS password fallback.
   - In the RADIUS section, clear the **PasswordFallbackEnabled** checkbox. to disable RADIUS password fallback.
6. Perform one of the following:
   - In the RADIUS section, select the **DynAuthReplayProtection** checkbox, to enable RADIUS replay protection.
   - In the RADIUS section, clear the **DynAuthReplayProtection** checkbox, to disable RADIUS replay protection .
7. In the RADIUS Reachability section, click a **RadiusReachability** radio button.
8. In the RADIUS Reachability section, type the reachability user name in the **UserName** dialog box.
9. In the RADIUS Reachability section, type the reachability password in the **Password** dialog box.
10. In the RADIUS Reachability section, type the reachability password again to confirm in the **Confirm Password** dialog box.
11. In the RADIUS Reachability section, specify the time-out period in the **Timeout** dialog box.
12. In the RADIUS Reachability section, specify the number of retry attempts in the **Retry** dialog box.
13. In the RADIUS Reachability section, specify the interval between checks when the RADIUS server is unreachable in the **BadTimer** dialog box.
14. In the RADIUS Reachability section, specify the interval between checks when the RADIUS server is reachable in the **GoodTimer** dialog box.
15. In the RADIUS Accounting section, select the **InterimUpdates** checkbox to enable or disable RADIUS accounting interim updates for the switch.
16. In the RADIUS Accounting section, specify the time interval before RADIUS accounting interim updates times out in the **InterimUpdatesInterval** dialog box.
17. In the RADIUS Accounting section, click an **InterimUpdatesIntervalSource** radio button.
18. On the toolbar, click **Apply**.

Globals Tab Field Descriptions

Use the data in the following table to use the **Globals** tab.

Name	Description
UseMgmtIp	When selected, RADIUS uses the system management IP address as the source address for RADIUS requests.
PasswordFallbackEnabled	When selected, enables RADIUS password fallback.
DynAuthReplayProtection	When selected, enables RADIUS replay protection.
Reachability	Specifies the RADIUS server reachability mode. Values include: • **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 the reachability username.
Password	Specifies the reachability password.
Confirm Password	Verifies the reachability password.
Timeout	Specifies the time-out period. Values range from 1-60 seconds.
Retry	Specifes the number of retry attempts. Values range from 1-5 retries.
BadTimer	Specifies the interval between checks when the RADIUS server is unreachable. Values range from 30-600 seconds.
GoodTimer	Specifies the interval between checks when the RADIUS server is reachable. Values range from 30-600 seconds.
InterimUpdates	Enables or disables RADIUS accounting interim updates for the switch.
InterimUpdatesInterval	Specifies the time interval (in seconds) before RADIUS accounting interim updates times out. Values range from 60–3600 seconds. The default is 600 seconds.
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

Adding a MAC address to the allowed non-EAP MAC address list using EDM

Use this procedure to add a MAC address to the allowed non-EAP MAC address list. The new entry authorizes designated non-EAPOL clients to access the port.

Procedure

1. From the **Device Physical View**, right-click a port.
2. From the menu, click **Edit**.
3. In the work area, click the **EAPOL Advance** tab.
4. On the tool bar, click the **Non-EAP MAC** button.
5. On the tool bar, click **Insert** to open the Insert Allowed non-EAP MAC dialog.
6. Enter a MAC address in the **ClientMACAddr** box.
7. Click **Insert** to return to the Allowed non-EAP MAC tab.
8. On the Allowed non-EAP MAC toolbar, click **Apply**.

Allowed non-EAP MAC Tab Field Descriptions

Use the data in the following table to use the **Allowed non-EAP MAC** tab.

Name	Description
PortNumber	The port number in use.
ClientMACAddr	The MAC address of the client.

Deleting a MAC address from the allowed non-EAP MAC address list using EDM

Use this procedure to delete a MAC address from the allowed non-EAP MAC address list. When you delete the selected MAC address you remove authorized access to the port for designated non-EAPOL clients.

Procedure

1. From the **Device Physical View**, right-click a port.
2. From the menu, click **Edit** .
3. In the work area, click the **EAPOL Advance** tab.
4. On the tool bar, click the **Non-EAP MAC** button to open the Allowed non-EAP MAC tab.
5. In the table, click a row to delete.
6. On the toolbar, click **Delete**.

7. Click **Yes** to delete the entry and return to the Allowed non-EAP MAC tab.

Allowed non-EAP MAC Tab Field Descriptions

Use the data in the following table to use the **Allowed non-EAP MAC** tab.

Name	Description
PortNumber	The port number in use.
ClientMACAddr	The MAC address of the client.

Viewing port non-EAP host support status using EDM

Use this procedure to view non-EAP host support status for a port.

Procedure

1. From the **Device Physical View**, right-click a port.
2. From the menu, click **Edit** .
3. In the work area, click the **EAPOL Advance** tab.
4. On the tool bar, click the **Non-EAP MAC** button.
5. Click the **Non-EAP Status** tab.

Non-EAP Status Tab Field Descriptions

Use the data in the following table to use the **Non-EAP Status** tab.

Name	Description
PortNumber	The port number in use.
ClientMACAddr	The MAC address of the client.
State	The authentication status. Possible values are: • **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.

Table continues…

Name	Description
	• **mhsaAuthenticated**: the MAC address was auto-authenticated on a port following a successful authentication of an EAP client.
Reauthenticate	The value used to reauthenticate the MAC address of the client on the port.
Vid	Indicates the VLAN assigned to the client.
Pri	Indicates the priority of the client.

Graphing port EAPOL statistics using EDM

Use this procedure to create a graph of port EAPOL statistics.

Procedure

1. In the navigation tree, double-click **Graph** to open the Graph tree.
2. From the Graph tree, double-click **Port** .
3. In the work area, click the **EAPOL Stats** tab.
4. Click a row to graph.
5. From the toolbar, select a graph type to create a graph.

EAPOL Stats Tab Field Descriptions

Use the data in the following table to use the **EAPOL Stats** tab.

Name	Description
EapolFramesRx	The number of valid EAPOL frames of any type that are received by this authenticator.
EapolFramesTx	The number of EAPOL frame types of any type that are transmitted by this authenticator.
EapolStartFramesRx	The number of EAPOL start frames that are received by this authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that are received by this authenticator.
EapolRespIdFramesRx	The number of EAPOL Resp/Id frames that are received by this authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (Other than Resp/Id frames) that are received by this authenticator.
EapolReqIdFramesTx	The number of EAPOL Req/Id frames that are transmitted by this authenticator.

Table continues…

Name	Description
EapolReqFramesTx	The number of EAP Req/Id frames (Other than Req/Id frames) that are transmitted by this authenticator.
InvalidEapolFramesRx	The number of EAPOL frames that are received by this authenticator in which the frame type is not recognized.
EapLengthErrorFramesRx	The number of EAPOL frames that are received by this authenticator in which the packet body length field is not valid.

Graphing port EAPOL diagnostics using EDM

Use this procedure to create a graph of port EAPOL diagnostic statistics.

Procedure

1. In the navigation tree, double-click **Graph** to open the Graph tree.
2. From the Graph tree, click **Port**.
3. In the work area, click the **EAPOL Diag** tab.
4. Click a row to graph.
5. From the toolbar, click a graph type to create the graph.

EAPOL Diag Tab Field Descriptions

Use the data in the following table to use the **EAPOL Diag** tab.

Name	Description
EntersConnecting	Counts the number of times that the state machine transitions to the connecting state from any other state.
EapLogoffsWhileConnecting	Counts the number of times that the state machine transitions from connecting to disconnecting because of receiving an EAPOL-Logoff message.
EntersAuthenticating	Counts the number of times that the state machine transitions from connecting to authenticating, because of an EAP-Response or Identity message being received from the Supplicant.
AuthSuccessWhileAuthenticating	Counts the number of times that the state machine transitions from authenticating to authenticated, because of the Backend Authentication state machine indicating a successful authentication of the Supplicant.

Table continues…

Name	Description
AuthTimeoutsWhileAuthenticating	Counts the number of times that the state machine transitions from authenticating to aborting, because of the Backend Authentication state machine indicating an authentication timeout.
AuthFailWhileAuthenticating	Counts the number of times that the state machine transitions from authenticating to held, because of the Backend Authentication state machine indicating an authentication failure.
AuthReauthsWhileAuthenticating	Counts the number of times that the state machine transitions from authenticating to aborting, because of a reauthentication request.
AuthEapStartsWhileAuthenticating	Counts the number of times that the state machine transitions from authenticating to aborting, because of an EAPOL-Start message being received from the Supplicant.
AuthEapLogoffWhileAuthenticating	Counts the number of times that the state machine transitions from authenticating to aborting, because of an EAPOL-Logoff message being received from the Supplicant.
AuthReauthsWhileAuthenticated	Counts the number of times that the state machine transitions from authenticated to connecting, because of a reauthentication request.
AuthEapStartsWhileAuthenticated	Counts the number of times that the state machine transitions from authenticated to connecting, because of an EAPOL-Start message being received from the Supplicant.
AuthEapLogoffWhileAuthenticated	Counts the number of times that the state machine transitions from authenticated to disconnected, 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

Table continues…

Name	Description
	the Supplicant. Indicates that the Authenticator chooses an EAP-method.
BackendNonNakResponsesFromSupplicant	Counts the number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK. Indicates that the Supplicant can respond to the EAP-method that the Authenticator chooses.
BackendAuthSuccesses	Counts the number of times that the state machine receives an EAP-Success message from the Authentication Server. Indicates that the Supplicant has successfully authenticated to the Authentication Server.
BackendAuthFails	Counts the number of times that the state machine receives an EAP-Failure message from the Authentication Server. Indicates that the Supplicant has not authenticated to the Authentication Server.

Chapter 9: 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 fundamentals

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

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

How RADIUS works

A RADIUS application has two components:

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

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

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

RADIUS server configuration

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

Provide each user with the appropriate level of access.

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

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

RADIUS EAP or non-EAP requests to different servers

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

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

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

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

RADIUS servers with MHSA mode

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

Note:

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

RADIUS server priority in MHSA mode

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

- EAP RADIUS server – primary

- EAP RADIUS server – secondary

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

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

Note:

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

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 through CLI.

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

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

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 is not 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 might mark the server as reachable after a successful response from a ping, but the RADIUS Service might not be started on the server side.

RADIUS password fallback

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

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

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

The RADIUS password fallback feature is enabled by default.

RADIUS Interim Accounting Updates support

With RADIUS Interim Accounting Updates support enabled, the RADIUS server can make policy decisions based on real-time network attributes transmitted by the NAS.

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

RADIUS Interim Accounting Updates support is not enabled by default.

RADIUS Request use Management IP Address

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

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

When the switch operates in Layer 3 mode, by default, a RADIUS request uses one of the routing IP addresses on the switch. RADIUS Request use Management VLAN IP configuration ensures that

the switch or stack generates RADIUS requests using the source IP address of the management VLAN. In some customer networks, the source IP in the RADIUS request is used to track management access to the switch, or it can be used when non-EAP is enabled. Because non-EAP can use an IP in the password mask it is important to have a consistent IP address.

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

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

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

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

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-Based Network Security Configuration using CLI

This section describes the procedures you can use to configure RADIUS-based network security using CLI.

Configuring RADIUS Interim Accounting Updates support

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Disabling RADIUS Interim Accounting Updates support

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Configuring RADIUS Interim Accounting Updates support defaults

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

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

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

Variable definitions

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

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

Viewing RADIUS Interim Accounting Updates support status

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

Procedure

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

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

Example

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

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

Enabling RADIUS request use of Management IP

Use the following procedure to enable the user of Management VLAN IP by RADIUS requests using CLI.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

   OR

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

Disabling RADIUS request use of Management IP

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Viewing RADIUS request use Management IP status

Procedure

1. Log on to CLI to enter User EXEC mode.

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

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

Configuring switch RADIUS server settings

Use the following procedure to secure the network against unathorized access by configuring the server and client to authenticate user identities through a central database.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Variable definitions

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

Variable	Value
<ipaddr>	Specifies the IPv4 address of the primary server you want to add or configure. **Important:** A value of 0.0.0.0 indicates that a primary RADIUS server is not configured.
<ipv6addr>	Specifies the IPv6 address of the primary server you want to add or configure. **Important:** A value of 0.0.0.0 indicates that a primary RADIUS server is not configured.
default	Restores the switch RADIUS server settings to default values. To delete a RADIUS server and restore default RADIUS settings, use one of the following commands in the Global or Interface Command mode: • `default radius server host` • `default radius server host secondary`

Table continues…

Variable	Value
	• `default radius server host used-by eapol` • `default radius server host secondary used-by eapol` • `default radius server host used-by non-eapol` • `default radius server host secondary used-by non-eapol`
key <*key*>	Specifies the secret authentication and encryption key used for all communications between the NAS and the RADIUS server. The key, also referred to as the shared secret, must be the same as the one defined on the server. You are prompted to enter and confirm the key.
no	Deletes switch RADIUS server settings.
port <*port*>	Specifies the UDP port number for clients to use when trying to contact the RADIUS server at the corresponding RADIUS server IP address. RANGE: 1 to 65535 DEFAULT port number: 1812
retry <*1–5*>	Specifies the number of RADIUS retry attempts for a RADIUS Server instance. RANGE: 1 to 5
secondary	Specifies the RADIUS server you are configuring as the secondary server. The system uses the secondary server only if the primary server is not configured or is not reachable.
timeout <*timeout*>	Specifies the timeout interval between each retry for service requests to the RADIUS server. RANGE: 1 to 60 seconds DEFAULT: 2 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. If you do not specify the RADIUS server as either EAP or Non-EAP, the system configures the server as a Global RADIUS Server, and processes client

Table continues…

Variable	Value
	requests without designating them as separate EAP or Non-EAP.

Enabling or disabling RADIUS password fallback

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

Procedure

1. Enter VLAN Interface Configuration mode:

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

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

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

   OR

   To disable RADIUS password fallback, enter the following command:

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

Viewing RADIUS information

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show radius-server
   ```

Example

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

```
Switch#show radius-server
RADIUS Global Server
----------------------------------------------------------------
Primary Host           : 0.0.0.0
Secondary Host         : 0.0.0.0
Port                   : 1812
Time-out               : 2
Key                    : ***************
Radius Retry Limit     : 3

RADIUS EAP Server
```

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

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

Configuring RADIUS server reachability

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

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

   ```
   [default] radius reachability {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

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

Variable	Value
default	Restores RADIUS server reachability to default values.
password <*password*>	Specifies a password for the RADIUS request.
use-icmp	Uses ICMP packets to determine reachability of the RADIUS server (default).
use-radius	Uses dummy RADIUS requests to determine reachability of the RADIUS server.
username <*username*>	Specifies a user name for the RADIUS request.
timeout <1-60>	Sets the time-out period. Range is 1 to 60 seconds.

Table continues…

Variable	Value
retry <1-5>	Specifies the number of retry attempts. Range is from 1 to 5.
check	Initiates an immediate check to determine the reachability of the RADIUS server.
eap	Checks the EAP RADIUS server reachability.
bad-timer <30-600>	Sets the interval between checks when the RADIUS server is unreachable. Range is 30 to 600 seconds.
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

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show radius reachability
   ```

Example

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

```
Switch#show radius reachability
RADIUS reachability: USE ICMP
RADIUS reachability timeout: 10
RADIUS reachability retry: 3
RADIUS reachability bad timer: 60
RADIUS reachability good timer: 180
```

RADIUS-based Network Security Configuration using EDM

This section describes the procedures you can use to configure RADIUS-based Network Security Configuration using EDM.

Configuring the Global RADIUS Server using EDM

Use this procedure to configure the RADIUS server globally for processing client requests without designating separate EAP or Non-EAP.

Note:

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

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, double-click **RADIUS**.
3. In the work area, click the **Global RADIUS Server** tab.
4. Select an IPv4 or IPv6 address type in the **PrimaryRadiusServerAddressType** box.
5. Type an IPv4 or IPv6 address in the **PrimaryRadiusServer** field.
6. Select an IPv4 or IPv6 address type in the **SecondaryRadiusServerAddressType** box.
7. Type an IPv4 or IPv6 address in the **SecondaryRadiusServer** field.
8. Type a UDP port number in the **RadiusServerUdpPort** field.
9. Type a timeout value in the **RadiusServerTimeout** field.
10. To change the shared secret key, type a value in the **SharedSecret(Key)** field.
11. Confirm the new shared secret key value in the **ConfirmSharedSecret(Key)** field.
12. Type a value in the **RetryLimit** field.
13. On the toolbar, click **Apply**.

Global RADIUS Server Tab Field Descriptions

Use the data in the following table to use the **Global RADIUS Server** tab.

Name	Description
PrimaryRadiusServerAddressType	Specifies the IP address type for the primary Global RADIUS server. Values include unknown, IPv4, and IPv6.
PrimaryRadiusServer	Specifies the IPv4 or IPv6 address of the primary Global RADIUS server (default: 0.0.0.0). **Important:** An IPv4 address of 0.0.0.0 or an IPv6 address of 00:00:00:00:00:00:00:00 indicates that a

Table continues…

Name	Description
	primary Global RADIUS Server is not configured.
SecondaryRadiusServerAddressType	Specifies the IP address type for the secondary Global RADIUS server. Values include unknown, IPv4, and IPv6.
SecondaryRadiusServer	Specifies the IPv4 or IPv6 address of the secondary Global RADIUS server (default: 0.0.0.0). The secondary Global RADIUS server is used if the primary Global RADIUS server is unavailable or unreachable. **Important:** An IPv4 address of 0.0.0.0 or an IPv6 address of 00:00:00:00:00:00:00:00 indicates that a secondary Global RADIUS Server is not configured.
RadiusServerUdpPort	Specifies the UDP port number clients use to contact the Global RADIUS Server at the Global RADIUS Server IP address. RANGE: 1 to 65535 DEFAULT: 1812
RadiusServerTimeout	Specifies the timeout interval between each retry for service requests to the Global RADIUS server. DEFAULT: 2 seconds RANGE: 1 to 60 seconds
SharedSecret(key)	Specifies the value for the Global RADIUS Server shared secret key. **Important:** The shared secret key has a maximum of 16 characters.
ConfirmedSharedSecret(key)	Confirms the value of the shared secret key specified in the SharedSecret(Key) field. Entering a value in this field is only required if you changed the SharedSecret(Key).
RetryLimit	Specifies the number of RADIUS retry attempts for a Global RADIUS Server instance. RANGE: 1 to 5

Configuring the EAP RADIUS Server using EDM

Use this procedure to configure an EAP RADIUS Server for processing EAP client requests only.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, double-click **RADIUS**.
3. In the work area, click the **EAP RADIUS Server** tab.
4. Select an IPv4 or IPv6 address type in the **PrimaryRadiusServerAddressType** field.
5. Type an IPv4 or IPv6 address in the **PrimaryRadiusServer** box.
6. Select an IPv4 or IPv6 address type in the **SecondaryRadiusServerAddressType** field.
7. Type an IPv4 or IPv6 address in the **SecondaryRadiusServer** field.
8. Type a UDP port number in the **RadiusServerUdpPort** box.
9. Type a timeout value in the **RadiusServerTimeout** box.
10. To change the shared secret key, type a value in the **SharedSecret(Key)** box.
11. Confirm the new shared secret key value in the **ConfirmSharedSecret(Key)** box.
12. Perform one of the following:
    - To enable accounting, check the **AccountingEnabled** checkbox.
    - To disable accounting, clear the **AccountingEnabled** checkbox.
13. Type a value in the **AccountingPort** box.
14. Type a value in the **RetryLimit** field.
15. On the toolbar, click **Apply**.

EAP RADIUS Server Tab Field Descriptions

Use the data in the following table to use the **EAP RADIUS Server** tab.

Name	Description
PrimaryRadiusServerAddressType	Specifies the IP address type for the primary EAP RADIUS server. Values include IPv4 and IPv6.
PrimaryRadiusServer	Specifies the IPv4 or IPv6 address of the primary EAP RADIUS server (default: 0.0.0.0). **Important:** An IPv4 address of 0.0.0.0 or an IPv6 address of 00:00:00:00:00:00:00:00 indicates that a primary EAP RADIUS Server is not configured.
SecondaryRadiusServerAddressType	Specifies the IP address type for the secondary EAP RADIUS server. Values include IPv4 and IPv6.
SecondaryRadiusServer	Specifies the IPv4 or IPv6 address of the secondary EAP RADIUS server (default: 0.0.0.0). The

Table continues…

Name	Description
	secondary EAP RADIUS server is used if the primary EAP RADIUS server is unavailable or unreachable. **Important:** An IPv4 address of 0.0.0.0 or an IPv6 address of 00:00:00:00:00:00:00:00 indicates that a secondary EAP RADIUS Server is not configured.
RadiusServerUdpPort	Specifies the UDP port number clients use to contact the EAP RADIUS Server at the EAP RADIUS Server IP address. The port number can range between 1 and 65535, the default is 1812.
RadiusServerTimeout	Specifies the timeout interval between each retry for service requests to the EAP RADIUS server. The default is 2 Seconds. Value range of 1 to 60 seconds.
SharedSecret(key)	Specifies the value for the EAP RADIUS Server shared secret key. **Important:** The shared secret key has a maximum of 16 characters.
ConfirmedSharedSecret(key)	Confirms the value of the shared secret key specified in the SharedSecret(Key) field. Entering a value in this field is only required if you changed the SharedSecret(Key).
AccountingEnabled	Enables or disables RADIUS accounting for a Global RADIUS Server instance.
AccountingPort	Specifies the UDP accounting port number for clients to use when trying to contact the RADIUS server at the corresponding Global RADIUS Server IP address. Values range from 0 to 65535.
RetryLimit	Specifies the number of RADIUS retry attempts for a EAP RADIUS Server instance. Value range of 1 to 5.

Configuring the NEAP RADIUS Server using EDM

Use this procedure to configure an NEAP RADIUS Server for processing NEAP client requests only.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, double-click **RADIUS**.
3. In the work area, click the **NEAP RADIUS Server** tab.

4. Select an IPv4 or IPv6 address type in the **PrimaryRadiusServerAddressType** field.
5. Type an IPv4 or IPv6 address in the **PrimaryRadiusServer** box.
6. Select an IPv4 or IPv6 address type in the **SecondaryRadiusServerAddressType** field.
7. Type an IPv4 or IPv6 address in the **SecondaryRadiusServer** box.
8. Type a UDP port number in the **RadiusServerUdpPort** box.
9. Type a timeout value in the **RadiusServerTimeout** box.
10. To change the shared secret key, type a value in the **SharedSecret(Key)** box.
11. Confirm the new shared secret key value in the **ConfirmSharedSecret(Key)** box.
12. Perform one of the following:
    - To enable accounting, check the **AccountingEnabled** checkbox.
    - To disable accounting, clear the **AccountingEnabled** checkbox.
13. Type a value in the **AccountingPort** box.
14. Type a value in the **RetryLimit** box.
15. On the toolbar, click **Apply**.

NEAP RADIUS Server Tab Field Descriptions

Use the data in the following table to use the **NEAP RADIUS Server** tab.

Name	Description
PrimaryRadiusServerAddressType	Specifies the IP address type for the primary NEAP RADIUS server. Values include IPv4 and IPv6.
PrimaryRadiusServer	Specifies the IPv4 or IPv6 address of the primary NEAP RADIUS server (default: 0.0.0.0). **Important:** An IPv4 address of 0.0.0.0 or an IPv6 address of 00:00:00:00:00:00:00:00 indicates that a primary NEAP RADIUS Server is not configured.
SecondaryRadiusServerAddressType	Specifies the IP address type for the secondary NEAP RADIUS server. Values include IPv4 and IPv6.
SecondaryRadiusServer	Specifies the IPv4 or IPv6 address of the secondary NEAP RADIUS server (default: 0.0.0.0). The secondary NEAP RADIUS server is used if the primary NEAP RADIUS server is unavailable or unreachable.

Table continues…

Name	Description
	Important: An IPv4 address of 0.0.0.0 or an IPv6 address of 00:00:00:00:00:00:00:00 indicates that a secondary NEAP RADIUS Server is not configured.
RadiusServerUdpPort	Specifies the UDP port number clients use to contact the NEAP RADIUS Server at the NEAP RADIUS Server IP address. The port number can range between 1 and 65535, the default is 1812.
RadiusServerTimeout	Specifies the timeout interval between each retry for service requests to the NEAP RADIUS server. The default is 2 Seconds. Value range of 1 to 60 seconds.
SharedSecret(key)	Specifies the value for the NEAP RADIUS Server shared secret key. **Important:** The shared secret key has a maximum of 16 characters.
ConfirmedSharedSecret(key)	Confirms the value of the shared secret key specified in the SharedSecret(Key) field. Entering a value in this field is only required if you changed the SharedSecret(Key).
AccountingEnabled	Enables or disables RADIUS accounting for a Global RADIUS Server instance.
AccountingPort	Specifies the UDP accounting port number for clients to use when trying to contact the RADIUS server at the corresponding Global RADIUS Server IP address. Values range from 0 to 65535.
RetryLimit	Specifies the number of RADIUS retry attempts for a NEAP RADIUS Server instance. Value range of 1 to 5.

Viewing RADIUS Dynamic Authorization server information using EDM

Use this procedure to display RADIUS Dynamic Authorization server information for the switch.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Auth. Server** tab.

RADIUS Dynamic Auth. Server Tab Field Descriptions

Use the data in the following table to use the **RADIUS Dynamic Auth. Server** tab.

Name	Description
Identifier	Indicates the Network Access Server (NAS) identifier of the RADIUS Dynamic Authorization Server.
DisconInvalidClientAddresses	Indicates the number of Disconnect-Request packets received from unknown addresses.
CoAInvalidClientAddresses	Indicates the number of CoA-Request packets received from unknown addresses.

Configuring RADIUS parameters

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

Configuring RADIUS globally using EDM

Use this procedure to configure RADIUS security for the switch.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, double-click **RADIUS**.
3. In the work area, click the **Globals** tab.
4. Perform one of the following:
   - In the RADIUS section, select the **UseMgmtIp** checkbox, to enable RADIUS request use management.
   - In the RADIUS section, clear the **UseMgmtIp** checkbox, to disable RADIUS request use management.
5. Perform one of the following:
   - In the RADIUS section, select the **PasswordFallbackEnabled** checkbox, to enable RADIUS password fallback.
   - In the RADIUS section, clear the **PasswordFallbackEnabled** checkbox. to disable RADIUS password fallback.
6. Perform one of the following:
   - In the RADIUS section, select the **DynAuthReplayProtection** checkbox, to enable RADIUS replay protection.
   - In the RADIUS section, clear the **DynAuthReplayProtection** checkbox, to disable RADIUS replay protection .
7. In the RADIUS section, click a **RadiusReachability** radio button.

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

Global RADIUS Server Tab Field Descriptions

Use the data in the following table to use the **Global RADIUS Server** tab.

Name	Description
PrimaryRadiusServerAddressType	Specifies the IP address type for the primary Global RADIUS server. Values include unknown, IPv4, and IPv6.
PrimaryRadiusServer	Specifies the IPv4 or IPv6 address of the primary Global RADIUS server (default: 0.0.0.0). **Important:** An IPv4 address of 0.0.0.0 or an IPv6 address of 00:00:00:00:00:00:00:00 indicates that a primary Global RADIUS Server is not configured.
SecondaryRadiusServerAddressType	Specifies the IP address type for the secondary Global RADIUS server. Values include unknown, IPv4, and IPv6.
SecondaryRadiusServer	Specifies the IPv4 or IPv6 address of the secondary Global RADIUS server (default: 0.0.0.0). The secondary Global RADIUS server is used if the primary Global RADIUS server is unavailable or unreachable. **Important:** An IPv4 address of 0.0.0.0 or an IPv6 address of 00:00:00:00:00:00:00:00 indicates that a secondary Global RADIUS Server is not configured.
RadiusServerUdpPort	Specifies the UDP port number clients use to contact the Global RADIUS Server at the Global RADIUS Server IP address. RANGE: 1 to 65535 DEFAULT: 1812
RadiusServerTimeout	Specifies the timeout interval between each retry for service requests to the Global RADIUS server. DEFAULT: 2 seconds RANGE: 1 to 60 seconds
SharedSecret(key)	Specifies the value for the Global RADIUS Server shared secret key.

Table continues…

Name	Description
	Important: The shared secret key has a maximum of 16 characters.
ConfirmedSharedSecret(key)	Confirms the value of the shared secret key specified in the SharedSecret(Key) field. Entering a value in this field is only required if you changed the SharedSecret(Key).
RetryLimit	Specifies the number of RADIUS retry attempts for a Global RADIUS Server instance. RANGE: 1 to 5

802.1X dynamic authorization extension (RFC 5176) client configuration using EDM

Use the following procedures to create, delete, or modify a RADIUS Dynamic Authorization client configuration.

Configuring an 802.1X dynamic authorization extension (RFC 5176) client using EDM

Use this procedure to create and configure a RADIUS Dynamic Authorization client for the switch.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Auth. Client** tab.
4. On the tool bar, click **Insert**.
5. In the **Address** dialog box, type an IP address.
6. Perform one of the following:
   - To enable the RADIUS Dynamic Authorization client, select the **Enabled** checkbox.
   - To disable the RADIUS Dynamic Authorization client, clear the **Enabled** checkbox.
7. In the **UdpPort** dialog box, type a port number.
8. Perform one of the following:
   - To enable change of authorization request processing, select the **ProcessCoARequests** checkbox.
   - To disable change of authorization request processing, clear the **ProcessCoARequests** checkbox.

9. Perform one of the following:
   - To enable disconnect request processing, select the **ProcessDisconnectRequests** checkbox.
   - To disable disconnect request processing, clear the **ProcessDisconnectRequests** checkbox.
10. In the **Secret** dialog box, type a shared secret word.
11. In the **Confirm Secret** dialog box, retype the same shared secret word.
12. Click **Insert**.
13. On the toolbar, click **Apply**.

RADIUS Dynamic Auth. Client Tab Field Descriptions

Use the data in the following table to use the **RADIUS Dynamic Auth. Client** tab.

Name	Description
AddressType	Defines the IP address type of the RADIUS Dynamic Authorization Client.
Address	Defines the IP address of the RADIUS Dynamic Authorization Client.
Enabled	Enables or disables packet receiving from the RADIUS Dynamic Authorization Client.
UdpPort	Configures the server and NAS UDP port to listen for requests from the RADIUS Dynamic Authorization Client. Values range from 1025 to 65535.
ProcessCoARequests	Enables change-of-authorization (CoA) request processing.
ProcessDisconnectRequests	Enables disconnect request processing.
Secret	Configures the RADIUS Dynamic Authorization Client secret word.
ConfirmedSecret	Confirms the RADIUS Dynamic Authorization Client secret word.

Deleting an 802.1X dynamic authorization extension (RFC 5176) client configuration using EDM

Use this procedure to delete an existing RADIUS Dynamic Authorization client configuration.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Auth. Client** tab.
4. To select a RADIUS Dynamic Authorization client to delete, click the client row.

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

Modifying the 802.1X dynamic authorization extension (RFC 5176) client configuration using EDM

Use this procedure to edit an existing RADIUS Dynamic Authorization client configuration.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Auth. Client** tab.
4. To select a RADIUS Dynamic Authorization client to edit, click the client row.
5. In the client row, double-click the cell in the **Enabled** column.
6. Select a value from the list—**true** to enable RADIUS Dynamic Authorization client, or **false** to disable RADIUS Dynamic Authorization client for the VLAN.
7. In the client row, double-click the cell in the **UdpPort** column.
8. Edit the UDP port number as required.
9. In the client row, double-click the cell in the **ProcessCoARequests** column.
10. Select a value from the list—**true** to enable CoA request processing, or **false** to disable CoA request processing.
11. In the client row, double-click the cell in the **ProcessDisconnectRequests** column.
12. Select a value from the list—**true** to enable disconnect request processing, or **false** to disable disconnect request processing.
13. On the toolbar, click **Apply**.

RADIUS Dynamic Auth. Client Tab Field Descriptions

Use the data in the following table to use the **RADIUS Dynamic Auth. Client** tab.

Name	Description
AddressType	Indicates the IP address type for the RADIUS Dynamic Authorization Client. This is a read-only cell.
Address	Indicates the IP address of the RADIUS Dynamic Authorization Client. This is a read-only cell.
Enabled	Enables or disables packet receiving from the RADIUS Dynamic Authorization Client. • **enable**: True • **disable**: False

Table continues…

Name	Description
UdpPort	Defines the server and NAS UDP port to listen for requests from the RADIUS Dynamic Authorization Client. Values range from 1024 to 65535.
ProcessCoARequests	Enables or disables change of authorization (CoA) request processing.
ProcessDisconnectRequests	Enables or disables disconnect request processing.
Secret	The RADIUS Dynamic Authorization Client secret word. This cell remains empty.

Viewing the 802.1X dynamic authorization extension (RFC 5176) client information using EDM

Use this procedure to display existing RADIUS Dynamic Authorization client configurations for the switch.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Auth. Client** tab.

RADIUS Dynamic Auth. Client Tab Field Descriptions

Use the data in the following table to use the **RADIUS Dynamic Auth. Client** tab.

Name	Description
AddressType	Indicates the IP address type for the RADIUS Dynamic Authorization Client.
Address	Indicates the IP address of the RADIUS Dynamic Authorization Client.
Enabled	Indicates whether packet receiving from the RADIUS Dynamic Authorization Client is enabled (true) or disabled (false).
UdpPort	Indicates the server and NAS UDP port to listen for requests from the RADIUS Dynamic Authorization Client. Values range from 1024–65535.
ProcessCoARequests	Indicates whether change of authorization (CoA) request processing is enabled or disabled.
ProcessDisconnectRequests	Indicates whether disconnect request processing is enabled or disabled.
Secret	Indicates the secret word shared between the RADIUS Dynamic Authorization Client and the RADIUS server.

Editing the 802.1X dynamic authorization extension (RFC 5176) client secret word using EDM

Use this procedure to change the existing RADIUS Dynamic Authorization client secret word.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**
3. In the work area, click the **RADIUS Dynamic Auth. Client** tab.
4. On the tool bar, click **Change Secret**.
5. In the **Secret** dialog box, enter a new secret word.
6. In the **Confirmed Secret** dialog box, reenter the new secret word.
7. On the toolbar, click **Apply**.

Viewing RADIUS Dynamic Server statistics using EDM

Use this procedure to display RADIUS Dynamic Server statistical information.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Server Stats** tab.

RADIUS Dynamic Server Stats Tab Field Descriptions

Use the data in the following table to use the **RADIUS Dynamic Server Stats** tab.

Name	Description
ClientIndex	Indicates the RADIUS Dynamic Server client index.
ClientAddressType	Indicates the type of RADIUS Dynamic Server address. Values are ipv4 or ipv6.
ClientAddress	Indicates the IP address of the RADIUS Dynamic Server.
ServerCounterDiscontinuity	Indicates a count of RADIUS Dynamic Server discontinuity instances.

Graphing RADIUS Dynamic Server statistics using EDM

Use this procedure to display a graphical representation of statistics for a RADIUS Dynamic Server client.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **802.1X/EAP**.
3. In the work area, click the **RADIUS Dynamic Server Stats** tab.
4. To select a server, click the client row.
5. On the tool bar, click **Graph**.
6. Click **Line Chart**, **Area Chart**, **Bar Chart**, or **Pie Chart**.

Chapter 10: IPv6 First Hop Security

This chapter provides conceptual information and procedures to configure the IPv6 First Hop Security (FHS) using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

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.

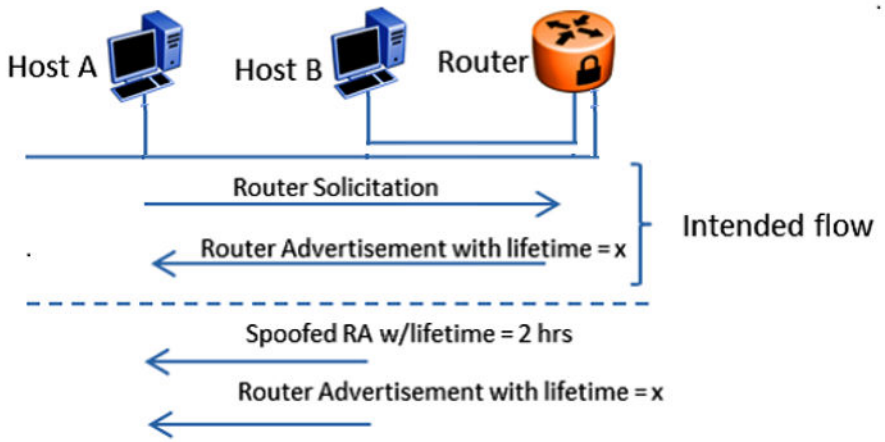

Figure 4: Message Flow IPv6 Router Discovery

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.

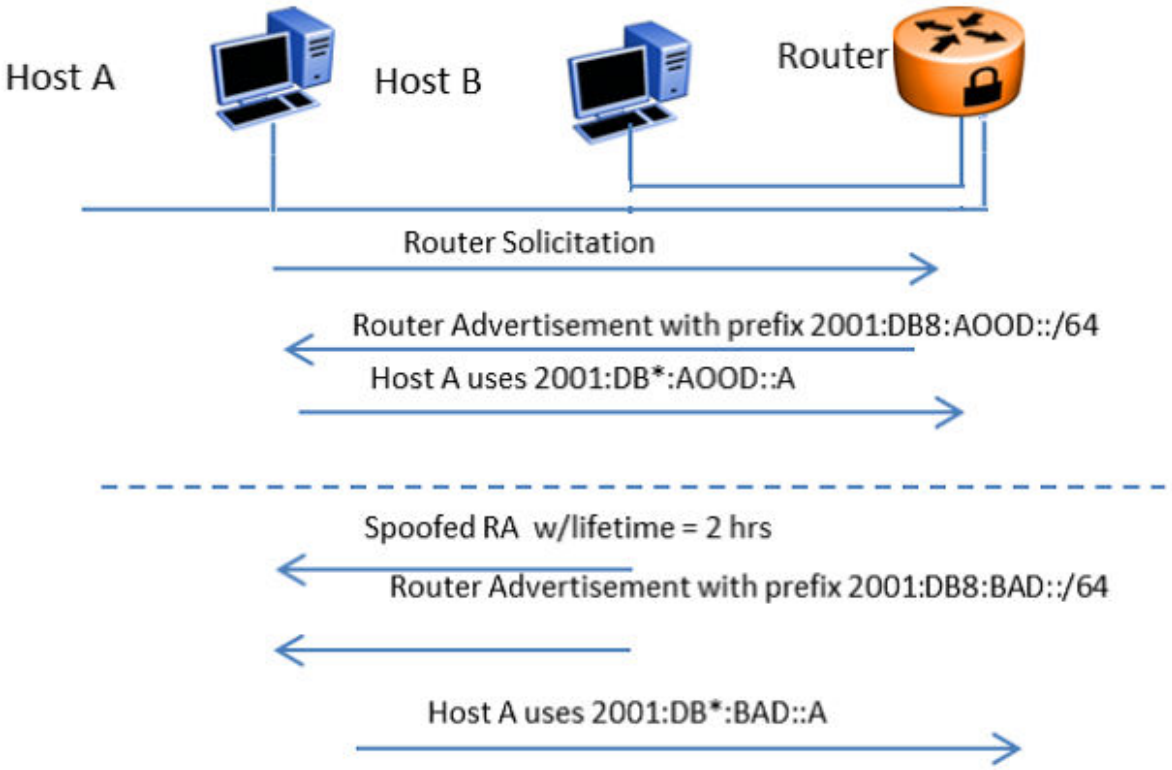

Figure 5: Stateless Address Autoconfiguration

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.

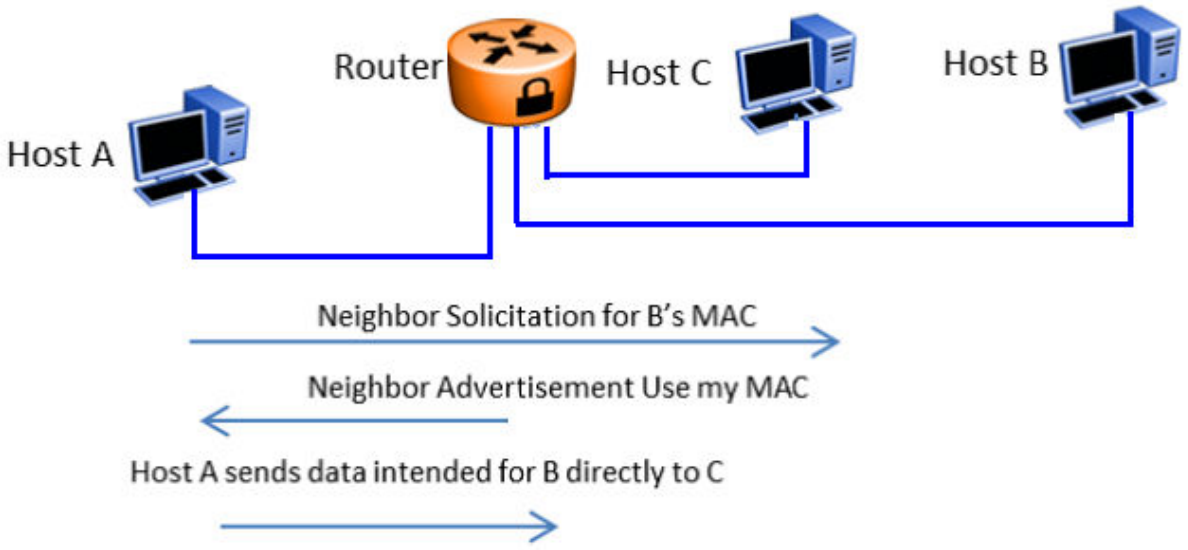

Figure 6: IPv6 Neighbor Discovery

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.

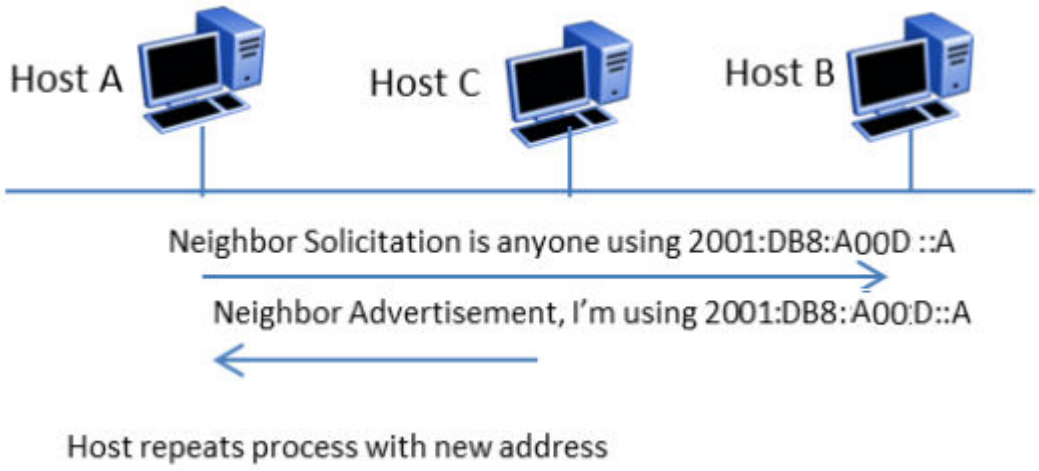

Figure 7: IPv6 Duplicate Address Detection

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.

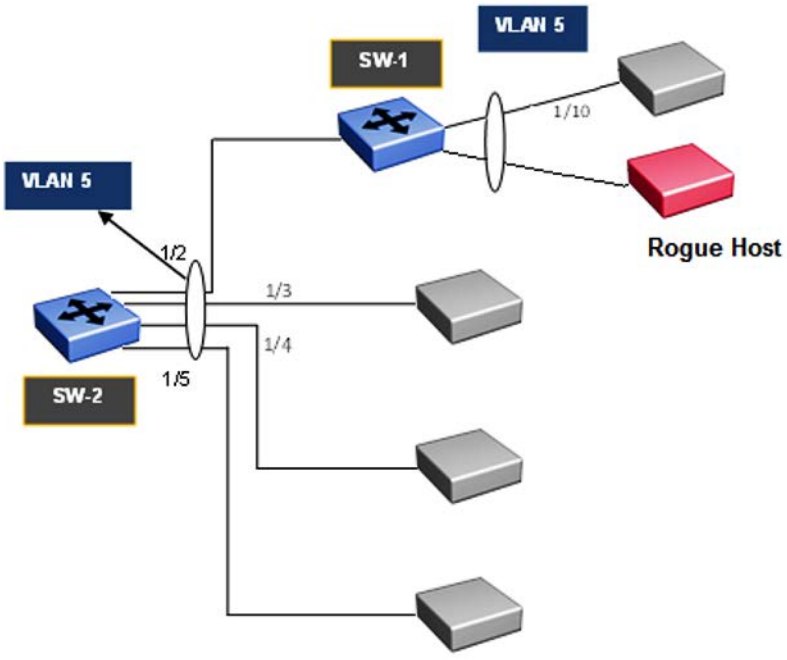

Figure 8: First Hop Security topology

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:

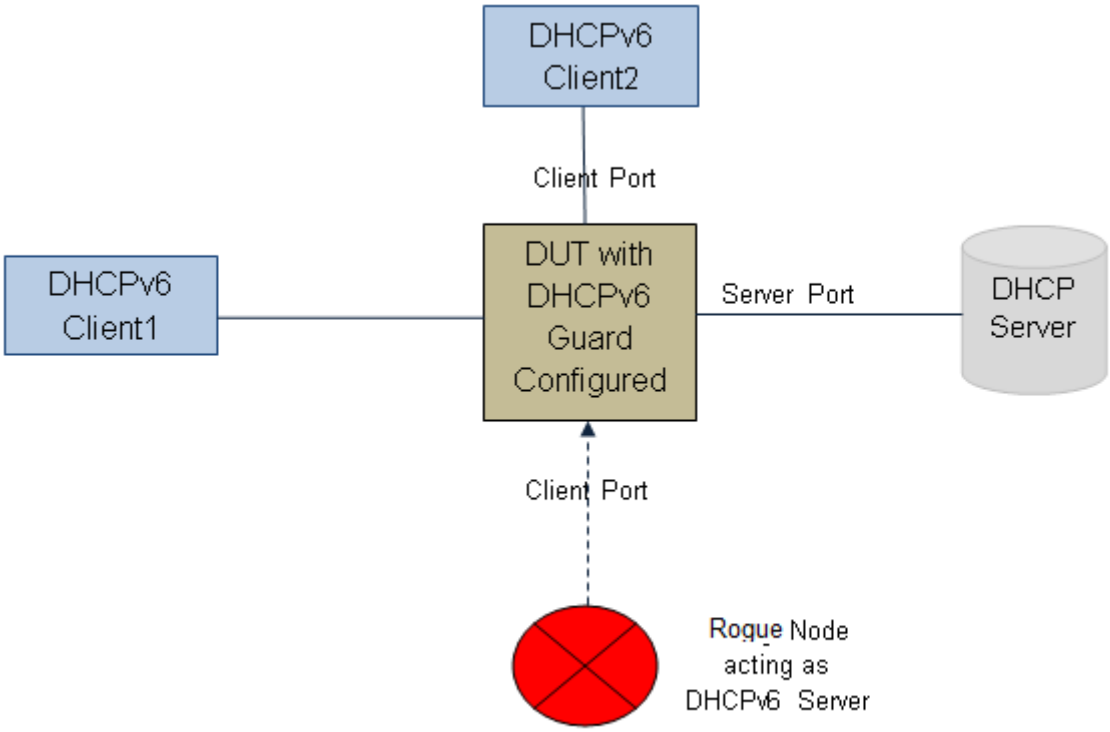

Figure 9: DHCPv6 Topology 1

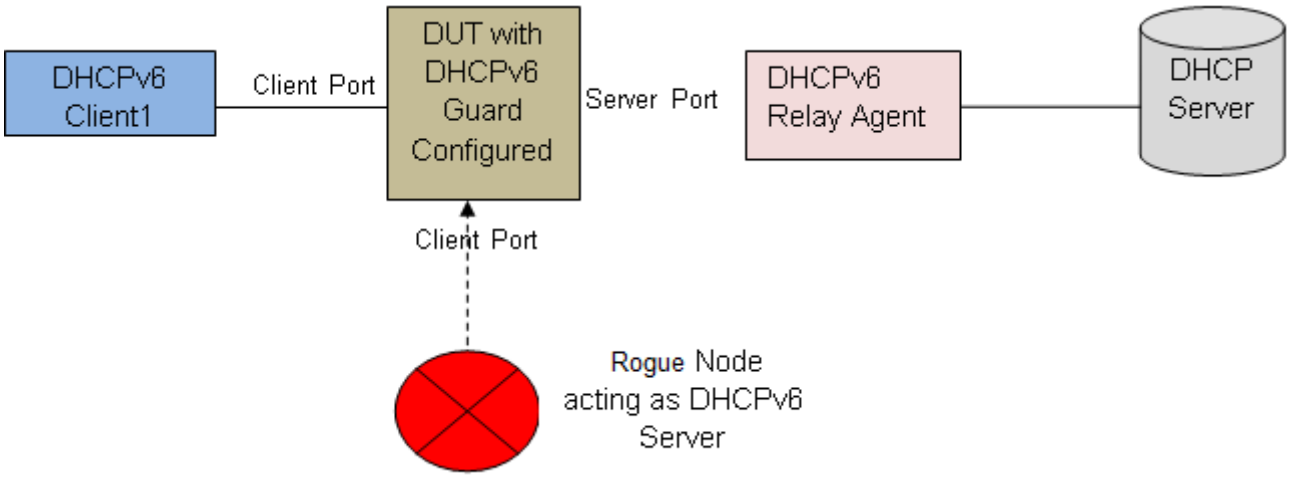

Figure 10: DHCPv6 Topology 2

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.

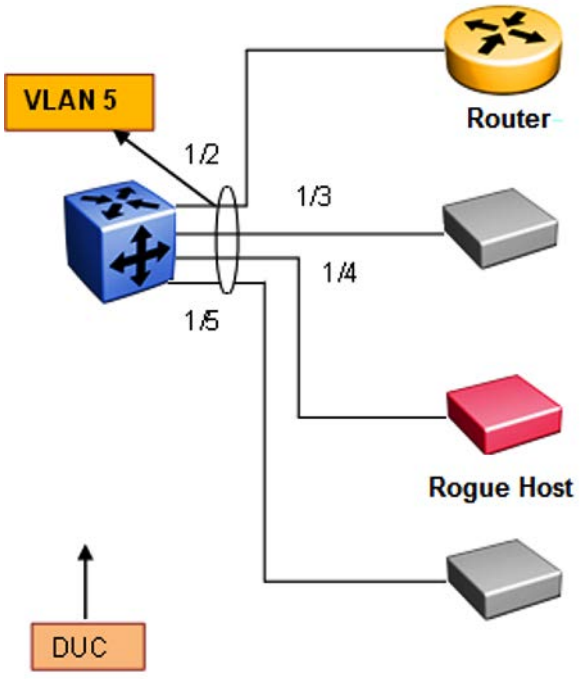

Figure 11: RA-guard Topology1

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.

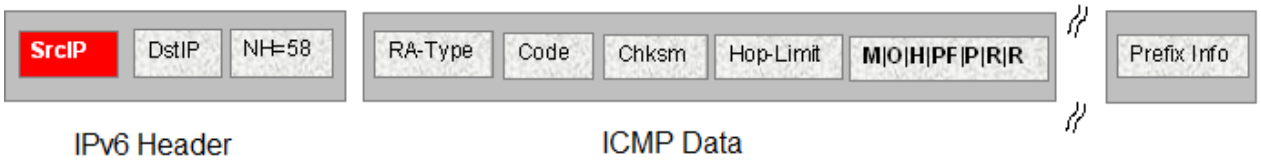

Figure 12: IPv6 ICMP RA data packet online

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.

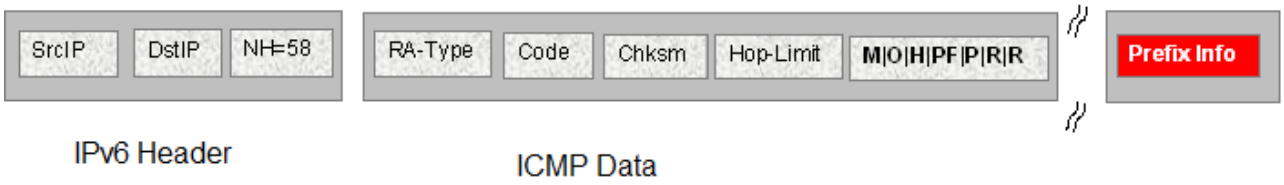

Figure 13: IPv6 ICMP RA data packet outline

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.

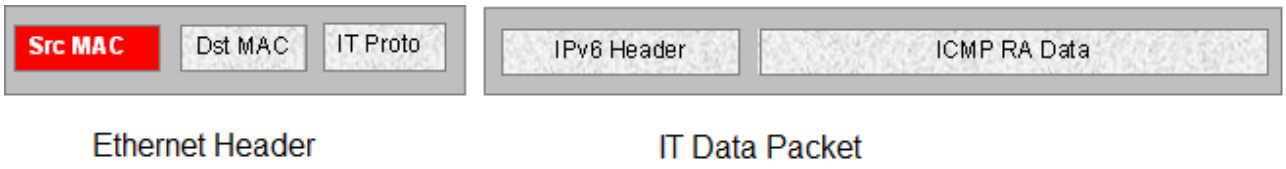

Figure 14: IPv6 Ethernet packet

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.

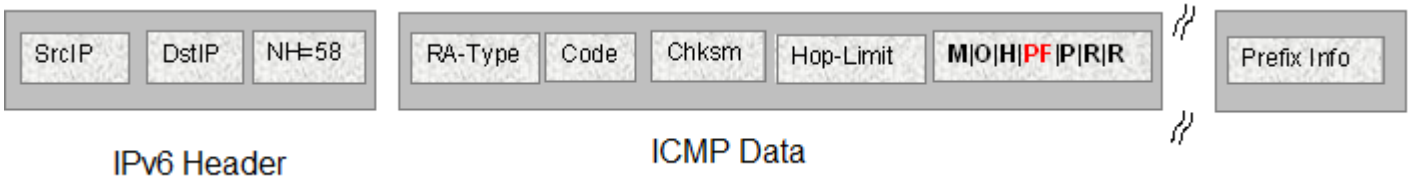

Figure 17: IPv6 ICMP RA data packet outline for router preference validation

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

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.

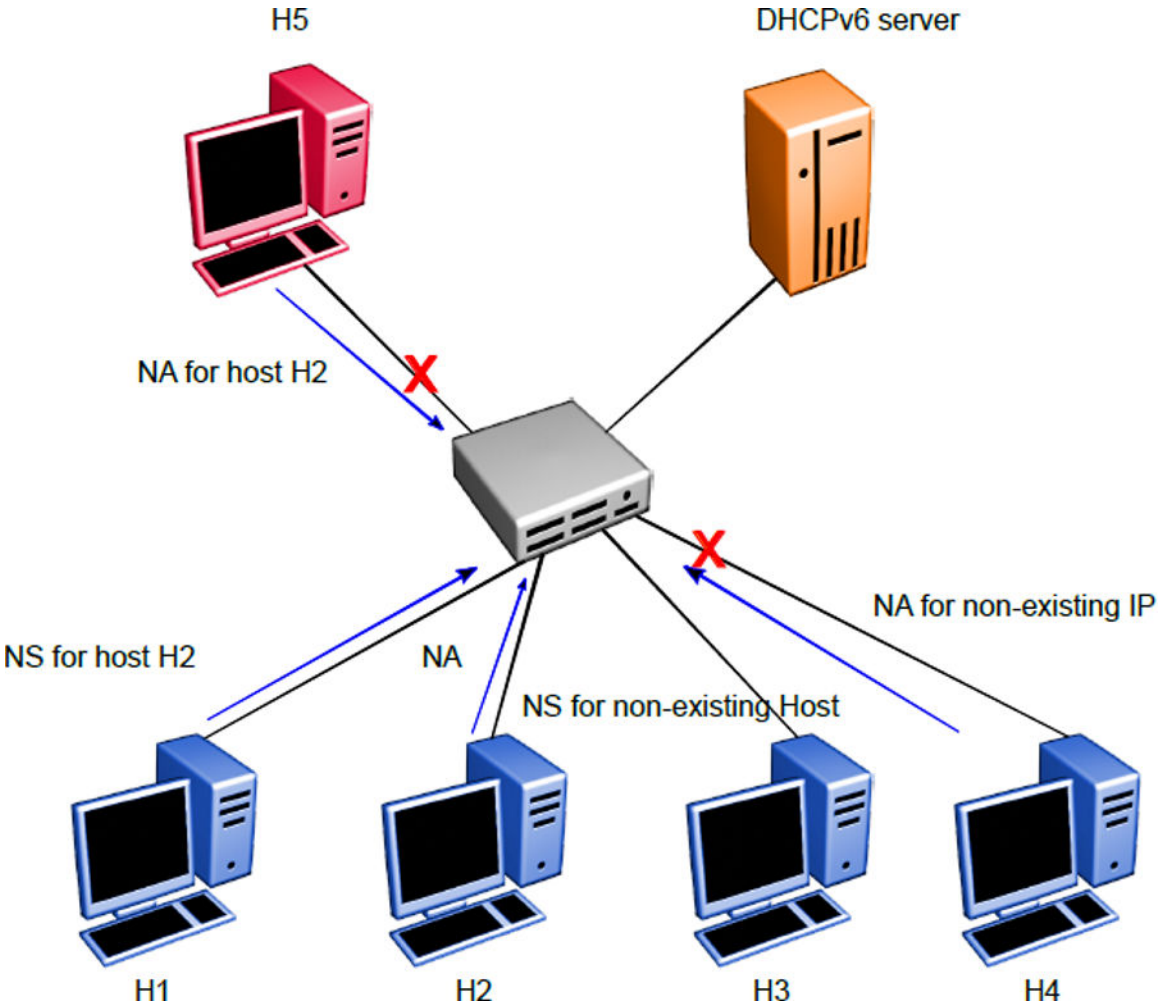

Figure 18: DAD/NUD/NS/NA attack prevention using ND-inspection

Table 3: 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

Capture 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.

Configuring IPv6 FHS using the 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.

Enable or Disable 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
   ```

Manage 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.

Display 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#
```

Manage 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

Display 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#
```

Display 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
```

Configuring DHCPv6–Guard Policy

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.

Enable or Disable 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
   ```

Manage 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.

Clear 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.

Manage 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.
{ 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.

Display 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. To enter User EXEC mode, log on to the switch.
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.

Configuring RA-Guard

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.

Enable or Disable 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
   ```

Manage 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.

Clear 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.

Manage 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.

Configure 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

Table continues…

Variable	Description
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. 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.

Display RA-Guard Configuration

About this task

Displays configured RA-guard policy information.

Procedure

1. To enter User EXEC mode, log on to the switch.
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.

Configuring ND-Inspection using the CLI

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.

Enable or Disable 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.

Manage 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. **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.

Manage 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

Table continues…

Variable	Description
	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. 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.

Clear 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.

Enable or Disable 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.

Table continues…

Variable	Description
	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 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.

Display ND-Inspection SBT Entries

About this task

Display SBT entries and other timer values.

Procedure

1. To enter User EXEC mode, log on to the switch.
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:

Extreme Networks recommends that you do 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::/32
1/3          fe80::210:94ff:fe00:550b
1/6          2000::10:10:0:2
```

IPv6 FHS configuration using EDM

This section describes how to configure IPv6 First Hop Security (FHS) 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.

Configure 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.

Globals Tab Field Descriptions

The following table describes the **Globals** tab.

Name	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.

Table continues…

Name	Description
SBTStaleLifeTime	Specifies the maximum STALE lifetime for a dynamically learnt SBT entry. 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.

Create 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**.

IP Access List Tab Field Descriptions

Use the data in the following table to use the **IP Access List** tab.

Name	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.

View 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.

IP Access List Tab Field Descriptions

Use the data in the following table to use the **IP Access List** tab.

Name	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.

Table continues…

Name	Description
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.

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.

Create 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**.

MAC Access List Tab Field Descriptions

Use the data in the following table to use the **MAC Access List** tab.

Name	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.

View 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.

MAC Access List Tab Field Descriptions

Use the data in the following table to use the **MAC Access List** tab.

Name	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.

Delete 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.

DHCPv6 Guard Policy Tab Field Descriptions

Use the data in the following table to use the **DHCPv6 Guard Policy** tab.

Name	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…

Name	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.

View 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.

DHCPv6 Guard Policy Tab Field Descriptions

Use the data in the following table to use the **DHCPv6 Guard Policy** tab.

Name	Description
PolicyName	Specify the policy name to create or modify DHCPv6-guard policy.

Table continues…

Name	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.

Delete 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**.

Create 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.

RA Guard Policy Tab Field Descriptions

The following table describes the **RA Guard Policy** tab fields.

Name	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.

Table continues…

Name	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 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. By default, none is selected and this check does not occur.
HopLimitMin	Specify the minimum hop limit to verify the advertised hop count limit.

Table continues…

Name	Description
	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.

View 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.

RA Guard Policy Tab Field Descriptions

The following table describes the **RA Guard Policy** tab fields.

Name	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

Table continues…

Name	Description
	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. 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.

Table continues…

Name	Description
	The value range is from 0 to 255 By default, maximum hop limit is 0 and the hop-limit check does not occur.

Delete 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**.

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.

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.

Create 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.

Port Policy Mapping Tab Field Descriptions

Use the data in the following table to use the **Port Policy Mapping** tab.

Name	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.

View 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.

Port Policy Mapping Tab Field Descriptions

Use the data in the following table to use the **Port Policy mapping** tab.

Name	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.

Table continues…

Name	Description
	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.

Delete 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.

Configure 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.

Source Binding Table Tab Field Descriptions

The following table describes the **Source Binding Table** tab.

Name	Description
InterfaceIndex	Specify the ports.
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.

View 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.

Source Binding Table Tab Field Descriptions

The following table describes the **Source Binding Table** tab.

Name	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.

Delete 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.

Configure 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**.

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.
ClearOverflowCount	Specifies whether the overflow counters must be cleared. By default, the value is false.

View 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 Tab Field Descriptions

Use the data in the following table to use the IPv6 **Source Guard Binding** tab.

Name	Description
IfIndex	Specifies a unique value assigned to each interface.
Ipv6Addr	Specifies binding entry for the IPv6 address

Chapter 11: 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 Unix systems, Windows systems, printers, modem racks, switches, routers, power supplies, Web servers, and databases. Any device that runs software that can retrieve SNMP information can be monitored.

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

SNMP Version 1 (SNMPv1)

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

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

SNMP Version 2 (SNMPv2)

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

SNMP Version 3 (SNMPv3)

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

Support for SNMP in the switch

The SNMP agent in the switch supports SNMPv1, SNMPv2c, and SNMPv3. Support for SNMPv2c provides 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, DES, and 3DES-based privacy encryption.

SNMP MIB support

SNMP agent with industry standard Management Information Bases (MIB) is supported, as well as private MIB extensions, which ensures compatibility with existing network management tools.

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

SNMP trap support

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

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

SNMP trap control

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

The following conditions apply to SNMP traps:

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

Per host notification control

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

Configuring SNMP using CLI

This section provides procedures to configuring SNMP using CLI.

Enabling or disabling the SNMP server

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Disabling SNMP access

Important:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   no snmp-server
   ```

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

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To enable the generation of SNMP authentication failure traps, enter the following command:

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

   OR

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

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

   OR

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

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

Modifying the community strings for SNMPv1 and SNMPv2c access

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

These community strings have a fixed MIB view.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

Variable	Value
<community-string>	Changes community strings for SNMPv1 and SNMPv2c access. Enter a community string that functions as a password and permits access to the SNMP protocol. If you set the value to **NONE**, it is disabled. **Important:** This parameter is not available when Password Security is enabled, in which case, the switch prompts you to enter and confirm the new community string.
ro | rw	Specifies read-only or read/write access. Stations with **ro** access can retrieve only MIB objects, and stations with **rw** access can retrieve and modify MIB objects. **Important:** If neither **ro** nor **rw** is specified, ro is assumed (default)

Clearing the SNMP server community configuration

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Restoring the community string configuration to default settings

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

If the read-only or read/write parameter is omitted from the command, all communities are restored to their default settings. The read-only community is set to **public**, the read/write community is set to **private** and all other communities are deleted.

Displaying SNMP community string configuration

Note:

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show snmp-server community
   ```

Configuring the SNMP sysContact value

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Clearing or restoring the SNMP sysContact value to default value

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To clear the sysContact value, enter the following command:

   ```
   no snmp-server contact
   ```

   OR

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

   ```
   default snmp-server contact
   ```

Configuring or clearing the SNMP sysLocation value

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. To configure the SNMP sysLocation value, enter the following command:

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

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

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

Variable definitions

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

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

Restoring the SNMP sysLocation to the default

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

```
default snmp-server location
```

Configuring the SNMP sysName value

Use the following procedure to configure the SNMP sysName value.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Variable definitions

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

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

Clearing the SNMP sysName value

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   no snmp-server name
   ```

   OR

   ```
   default snmp-server name
   ```

Enabling SNMP linkUp linkDown traps for a port

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

   or

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

Variable definitions

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

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

Disabling the SNMP linkUp linkDown traps for a port

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

   OR

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

   for linkUp trap.

   Or

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

   Or

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

   for linkDown trap.

Variable definitions

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

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

Adding SNMP traps to a filter profile

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

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

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

Variable definitions

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

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

Deleting SNMP traps from a filter profile

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

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

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

Variable definitions

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

Variable	Value
<filterName>	Specifies the filter profile name.
<WORD>	Specifies the description of OID specification of the SNMP trap added to the filterName filter. By default, each OID specified is included in the filter. To indicate that an OID is included in the filter,

Table continues…

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

Displaying notify-filter details

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Variable definitions

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

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

Enabling or disabling the generation of SNMP traps

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To enable the generation of SNMP traps, enter the following command:

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

   OR

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

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

Variable definitions

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

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

Creating an SNMPv3 user

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Table continues…

Variable	Value
md5/sha <*password*>	Specifies the use of an md5/sha authentication pass phrase. • *password*—specifies the new user md5 /sha authentication pass phrase; enter an alphanumeric string. If this parameter is omitted, the user is created with only unauthenticated access rights. **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.
read-view <*view-name*>	Specifies the read view to which the new user has access: • *view-name*—specifies the view name; enter an alphanumeric string of up to 255 characters.
write-view <*view-name*>	Specifies the write view to which the new user has access: • *view-name*—specifies the view name; enter an alphanumeric string of up to 255 characters.
notify-view <*view-name*>	Specifies the notify view to which the new user has access: • *view-name*— specifies the view name; enter an alphanumeric string of up to 255 characters.
des/aes/3des <*password*>	Specifies the use of a des/aes/3des privacy pass phrase. • password—specifies the new user des/aes/3des privacy pass phrase; enter an alphanumeric string of minimum 8 characters. If this parameter is omitted, the user is created with only authenticated access rights. **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.

The **sha** and **des** parameters are available only if the switch image has full SHA/DES support.

The command shows three sets of read/write/notify views. The first set specifies unauthenticated access. The second set specifies authenticated access. The third set specifies authenticated and encrypted access.

You can specify authenticated access only if the **md5** or **sha** parameter is included. Likewise, you can specify authenticated and encrypted access only if the **des**, **aes**, or **3des** parameter is included.

If you omit the authenticated view parameters, authenticated access uses the views specified for unauthenticated access. If you omit all the authenticated and encrypted view parameters, the authenticated and encrypted access uses the same views that are used for authenticated access. These views are the unauthenticated views, if all the authenticated views are also omitted.

Creating an SNMPv3 view

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

Variable	Value
<*viewname*>	Specifies the name of the new view; enter an alphanumeric string.
<*OID*>	Specifies the Object identifier. *OID* can be entered as a MIB object English descriptor, a dotted form *OID*, or a mix of the two. Each *OID* can also be preceded by a plus (+) or minus (–) sign (if the minus sign is omitted, a plus sign is implied). For the dotted form, a subidentifier can be an asterisk (*), which indicates a wildcard. Some examples of valid *OID* parameters are as follows: • **sysName** • **+sysName** • **-sysName** • **+sysName.0** • **+ifIndex.1**

Table continues…

Variable	Value
	• **-ifEntry.*.1** (matches all objects in the if Table with an instance of 1, that is, the entry for interface #1) • **1.3.6.1.2.1.1.1.0** (dotted form of **sysDescr**) The plus (+) or minus (–) sign indicates whether the specified *OID* is included in or excluded from, respectively, the set of MIB objects that are accessible by using this view. For example, if you create a view as follows: **snmp-server view myview +system -sysDescr** and you use that view for the read-view of a user, then the user can read only the system group, except for **sysDescr**.

Removing an SNMPv3 user

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Removing an SNMPv3 view

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Adding trap receivers to SNMPv3 tables

Use the following procedure to add a trap receiver to the SNMPv3 tables. You can create several entries in this table, and each can generate v1, v2c, or v3 traps. You can use notification filters to trap receivers and include SNMP traps in notification filters.

Before you begin

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

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

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

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

Variable definitions

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

Variable	Value
port *<1-65535>*	Sets the SNMP trap port.
A.B.C.D	Specifies the dotted-decimal IP address of a host to be the trap destination.
<community-string:WORD>	If you do not specify a trap type, this variable creates v1 trap receivers in the SNMPv3 MIBs. You can create multiple trap receivers with varying access levels.

Table continues…

Variable	Value
filter <*WORD*>	Specifies the filter profile name. The **snmp-server host** command is improved with the filter parameter only for the hosts with a specified SNMP version (v1/v2c/v3). Add the filter parameter only for the normal syntax form of the **snmp-server host** command. When you delete a specific SNMP-server host with the **no** command or delete all configured SNMP-server hosts with the **default** command, the associated filters are also deleted.
inform	Generates acknowledge inform requests.
<*ipv6addr*>	Specifies the IPv6 address of the SNMP notification host.
retries <*0-255*>	Specifies the number of retries for inform requests. RANGE: 0-2147483647
target-name <*WORD/1-32*>	Specifies the name of the target.
timeout <*1-2147483647*>	Specifies the timeout for inform requests. RANGE: 1-2147483647 centi-seconds
<*username:WORD*>	Specifies the SNMPv3 user name for trap destination; enter an alphanumeric string.
v1 <*community-string:WORD*>	Creates v1 trap receivers in the SNMPv3 MIBs. You can create multiple trap receivers with varying access levels.
v2c <*community-string:WORD*>	Creates v2c trap receivers in the SNMPv3 MIBs. You can create multiple trap receivers with varying access levels.
v3 {auth|no-auth| auth-priv}	Using v3 creates v3 trap receivers in the SNMPv3 MIBs. You can create multiple trap receivers with varying access levels by entering the following variables: • **auth|no-auth** —Specifies whether SNMPv3 traps can be authenticated. • **auth-priv**—This parameter is only available if the image has full SHA/DES support.

Deleting trap receivers or restoring the SNMPv3 table to defaults

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

Important:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

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

   ```
   default snmp-server host
   ```

Variable definitions

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

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

Displaying SNMP-server host-related information

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show snmp-server host
   ```

Example

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

```
Switch#show snmp-server host
-------------------------------------------------------------------------
Notify Group: inform
  Type         : Inform
  Storage Type: Read-Only
  Status       : Active

-------------------------------------------------------------------------
Notify Group: s5AgTrpRcvr
```

```
  Type         : Trap
  Storage Type: Read-Only
  Status       : Active

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



IPv6 Trap Destinations:

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

Setting SNMP community strings and access privileges

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

This command affects community strings stored in the SNMPv3 snmpCommunityTable, which allows several community strings to be created. These community strings can have any MIB view.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Variable definitions

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

Variable	Value
<community- string>	Enter a community string to be created with access to the specified views. **Important:** This parameter is not available when Password Security is enabled, in which case, the switch prompts you to enter and confirm the new community string.

Table continues…

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

Displaying SNMPv3 configuration

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

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

Variable definitions

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

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

Creating an initial set of configuration data for SNMPv3

Use the following procedure to create an initial set of configuration data for SNMPv3. This configuration data follows the conventions described in the SNMPv3 standard (in RFC 3414 and 3415). The data consists of a set of initial users, groups, and views.

Important:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

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

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

Configuring SNMP using EDM

This section provides procedures to configure SNMP using EDM.

Viewing SNMP information using EDM

Use this procedure to view read-only information about the addresses that the agent software uses to identify the switch.

Perform this procedure to view SNMP information.

Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree.
2. From the Edit tree, click **Chassis**.
3. In the Chassis tree, click **Chassis**.
4. In the work area, click the **SNMP** tab.

SNMP Tab Field Descriptions

Use the data in the following table to use the **SNMP** tab.

Name	Description
LastUnauthenticatedInetAddressType	The type of IP address that was not authenticated by the device last.
LastUnauthenticatedInetAddress	The last IP address that is not authenticated by the device.
LastUnauthenticatedCommunityString	The last community string that is not authenticated by the device.
RemoteLoginInetAddressType	Specifies either IPv4 or IPv6.
RemoteLoginInetAddress	Specifies the remote login IP address.
TrpRcvrMaxEnt	The maximum number of trap receiver entries.
TrpRcvrCurEnt	The current number of trap receiver entries.
TrpRcvrNext	The next trap receiver entry to be created.

Defining a MIB view using EDM

Use this procedure to assign MIB view access for an object.

Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **MIB View**.
4. On the toolbar, click **Insert**.
5. On the Insert MIB View dialog, enter and select criteria to describe the MIB View.

6. Click **Insert**.
7. On the toolbar, click **Apply**.

MIB View Tab Field Descriptions

Use the data in the following table to use the **MIB View** tab.

Name	Description
ViewName	Specifies a name for the new entry in a range from 1 to 32 characters.
Subtree	Specifies any valid object identifiers that define a set of MIB objects accessible by this SNMP entry. For example; ort, iso8802, or 1.3.5.1.1.5 OID string.
Type	To determine whether access to a MIB object is granted or denied, select one of the following: • **included**: Granted • **excluded**: Denied
Storage Type	Select one of the following: • **volatile**: Entry does not persist if switch loses power • **nonVolatile**: Entry persists if switch loses power

Configuring an SNMP user using EDM

Use this procedure to create an SNMP user.

Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **User**.
4. On the User tab tool bar, click **User**.
5. Click **Insert**.
6. Enter the parameters to describe the user.
7. Click **Insert**.
8. On the toolbar, click **Apply**.

User Tab Field Descriptions

Use the data in the following table to use the tab.

Name	Description
Engine ID	Indicates the administratively-unique identifier of the SNMP engine.
Name	Indicates the name of the user in usmUser.
Auth Protocol	Select an authentication protocol from the following list: • **None** • **MD5** • **SHA**
AuthPassword	Specifies the current authorization password.
ConfirmPassword	Reenter the password to confirm.
Priv Protocol	To assign a privacy protocol, select one of the following from the list: • **None** • **DES** • **3DES** • **AES**
PrivacyPassword	Specifies the current privacy password.
ConfirmPassword	Reenter the password to confirm.
ReadViewName	Specifies the name of the MIB View to which the user is assigned read access.
WriteViewName	Specifies the name of the MIB View to which the user is assigned write access.
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 SNMP user details using EDM

Use this procedure to view SNMP user details.

Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree
2. In the Edit tree, double-click **Snmp Server**.

3. In the Snmp Server tree, click **User**.
4. In the work area, on the User tab, select a user.
5. On the toolbar, click the **Details** button.

Configuring an SNMP community

A community string is a passphrase used by the switch in snmpv1 and snmpv2 operations. Use this procedure to configure an SNMP community string.

Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **Community**.
4. On the Community tab tool bar, click **Details**.
5. On the toolbar, click **Insert**.
6. Enter the parameters to describe the community.
7. Click **Insert**
8. On the toolbar, click **Apply**.

Community Tab Field Descriptions

Use the data in the following table to use the **Community** tab.

Name	Description
Index	Specifies the unique index value of a row in the community table.
Name	Specifies the community string: a row in the Community table represents a configuration.
ContextEngineId	Specifies the contextEngineID that indicates the location of the context in which management information is accessed when using the community string specified by the corresponding instance of CommunityName. The default value is the EngineID of the entity in which this object is represented.
CommunityString	Specifies a community string to be created with access to specific views. You can create community strings with varying levels of read, write, and notification access based on SNMPv3 views.
ReadView Name	Specifies the name of the MIB View to which the user is assigned read access.

Table continues…

Name	Description
WriteViewName	Specifies the name of the MIB View to which the user is assigned write access.
NotifyViewName	Specifies the name of the MIB View from which the user receives notifications.
Storage Type	If you need to describe a series of choices for the field, use an unordered list as follows: • **volatile**: Entry does not persist if switch loses power • **nonVolatile**: Entry persists if switch loses power

Viewing SNMP community details using EDM

Use this procedure to view SNMP community details.

Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **Community**.
4. In the work area, on the Community tab, select a community.
5. On the toolbar, click **Details**.

Configuring an SNMP host using EDM

Use this procedure to create an SNMP host.

Procedure

1. From the navigation tree, double-click **Edit** to open the navigation tree.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **Host**.
4. On the Host tab tool bar, click **Insert**.
5. On the Insert Host dialog, enter and select criteria to describe the host.
6. Click **Insert**.
7. On the toolbar, click **Apply**.

Insert Host Tab Field Descriptions

Use the data in the following table to use the **Insert Host** tab.

Name	Description
Domain	Select one of the following: • **IPv4** • **IPv6** The default value is IPv4.
DestinationAddr (Port)	Specifies the destination address, expressed in IPv4 Address : port format.
Timeout	Specifies the timeout interval, expressed in 1/100 of a second. The default value is 1500.
RetryCount	Specifies the number of retries the system attempts; expressed as an integer from 0 to 255. The default value is 3.
Type	Specifies the type as one of the following: • **trap** • **inform**
Version	Specifies the SNMP version as one of the following: • **SNMPv1** • **SNMPv2c** • **SNMPv3/USM**
SecurityName	Specifies security name used for generating SNMP messages.
SecurityLevel	Specifies the security level for SNMP messages as one of the following: • **noAuthNoPriv** • **authNoPriv** • **authPriv**
Storage Type	Select one of the following: • **volatile**: Entry does not persist if switch loses power • **nonVolatile**: Entry persists if switch loses power

Configuring SNMP host notification using EDM

Use this procedure to configure SNMP trap notification.

Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree.
2. In the Edit tree, double-click **Snmp Server**.

3. In the Snmp Server tree, click **Host**
4. On the Host tab tool bar, click **Notification**.
5. On the Insert Host dialog, enter and select criteria to describe the trap notification.
6. Click **Insert** to return to the Host tab.
7. On the toolbar, click **Apply**.

Host Tab Field Descriptions

Use the data in the following table to use the **Host** tab.

Name	Description
Domain	Indicates the address transport type; either IPv4 or IPv6.
DestinationAddr : Port	Indicates the transport address (in IPv4 Address : port format).
Timeout	Indicates the time interval that an application waits for a response in 1/100 second intervals from 0 to 2147483647.
RetryCount	Indicates the number of retries to be attempted when a response is not received for a generated message from 0 to 255.
Type	Indicates the type of the message; either trap or information.
Version	Indicates the SNMP version; either SNMPv1, SNMPv2c or SNMPv3/USM.
SecurityName	Enter the community string.
SecurityLevel	Indicates the security level; either no authorization and no priviliges, authorization and no privileges, or authorization and privileges.
StorageType	Select one of the following: • **volatile**: Entry does not persist if switch loses power • **nonVolatile**: Entry persists if switch loses power

Configuring SNMP notification control using EDM

Use this procedure to enable or disable SNMP traps in the list. Notification Control is the Trap Web Page.

Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **Notification Control**.

4. In the NotifyControlEnabled column, double-click the cell in the NotifyControlType (SNMP trap) row that you wish to modify.
5. Perform one of the following:
   - Select a value from the list: **true** to enable the SNMP trap.
   - Select a value from the list: **false** to disable SNMP trap.
   - On the toolbar, click the **Enable All** to enable all SNMP traps available on the switch.
   - On the toolbar, click the **Disble All** to disable all SNMP traps available on the switch.
6. On the toolbar, click **Apply**.

Notification Control Tab Field Descriptions

Use the data in the following table to use the **Notification Control** tab.

Name	Description
NotifyControlType	Lists the SNMP trap names.
Notify Control Type (oid)	Lists the object identifiers for the SNMP traps.
NotifyControlEnabled	Specifies whether traps are enabled or disabled.
NotifyControlPortListEnabled	Indicates the port list for which the notification is enabled or disabled. Whether or not this field is configurable is dependent on the NotifyControlType value.

Configuring SNMP notification control using EDM

Use this procedure to enable or disable SNMP traps in the list. Notification Control is the Trap Web Page.

Procedure

1. From the navigation tree, double-click **Edit** to open the Edit tree.
2. In the Edit tree, double-click **Snmp Server**.
3. In the Snmp Server tree, click **Notification Control**.
4. In the NotifyControlEnabled column, double-click the cell in the NotifyControlType (SNMP trap) row that you wish to modify.
5. Perform one of the following:
   - Select a value from the list: **true** to enable the SNMP trap.
   - Select a value from the list: **false** to disable SNMP trap.
   - On the toolbar, click the **Enable All** to enable all SNMP traps available on the switch.
   - On the toolbar, click the **Disble All** to disable all SNMP traps available on the switch.
6. On the toolbar, click **Apply**.

Notification Control Tab Field Descriptions

Use the data in the following table to use the **Notification Control** tab.

Name	Description
NotifyControlType	Lists the SNMP trap names.
Notify Control Type (oid)	Lists the object identifiers for the SNMP traps.
NotifyControlEnabled	Specifies whether traps are enabled or disabled.
NotifyControlPortListEnabled	Indicates the port list for which the notification is enabled or disabled. Whether or not this field is configurable is dependent on the NotifyControlType value.

Chapter 12: 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 is the ability of an attacker to respond to DHCP requests with false IP information. DHCP snooping acts like a firewall between untrusted hosts and the DHCP servers, so that DHCP spoofing cannot occur.

DHCP snooping classifies ports in the following two types:

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

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

- DHCP snooping allows only DHCP requests from untrusted ports. DHCP replies and all other types of DHCP messages from untrusted ports are dropped.
- DHCP snooping verifies the source of DHCP packets.
  - When the switch receives a DHCP request on an untrusted port, DHCP snooping compares the source MAC address and the DHCP client hardware address. If the addresses match, the switch forwards the packet. If the addresses do not match, the switch drops the packet.
  - When the switch receives a DHCP release or DHCP decline broadcast message from a client, DHCP snooping verifies that the port on which the message was received matches the port information for the client MAC address in the DHCP binding table. If the port information matches, the switch forwards the DHCP packet.

DHCP binding table

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

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

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

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

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

DHCP snooping configuration and management

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

Configure and manage DHCP snooping by using the Command Line Interface (CLI), Enterprise Device Manager (EDM), and SNMP.

DHCP snooping Global Configuration

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

DHCP Option 82

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

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

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

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

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

For more information about DHCP Option 82 with DHCP relay, see Configuring IP Routing and Multicast on Ethernet Routing Switch 3600 Series .

Configuring DHCP Snooping using CLI

This section provides procedures to configure DHCP snooping using CLI.

Configuring DHCP snooping globally

Configure DHCP snooping globally for DHCP snooping to be functional at the VLAN and port level on the switch. By default DHCP snooping is disabled globally.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Configuring DHCP snooping on a VLAN

Enable DHCP snooping on a VLAN for DHCP snooping to be functional on the VLAN. You must enable DHCP snooping separately for each VLAN as required.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Configuring DHCP snooping port trust

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

Procedure

1. Enter Interface Configuration mode:

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

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

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

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

   ```
   default ip dhcp-snooping port all
   ```

Variable definitions

The following table describes the parameters for the **`ip dhcp-snooping`** command.

Variable	Value
[default]	Returns a port or range of ports to default DHCP snooping values.
[no]	Removes the Option 82 for DHCP snooping subscriber Id from a port.
option82-subscriber-id <WORD>	Specifies the DHCP Option 82 subscriber Id for the port. Value is a character string between 0 and 64 characters.
<portlist>	Specifies a port or group of ports.
<trusted>	When selected, the port or ports automatically forward DHCP replies.
<untrusted>	When selected, the port or ports filter DHCP replies through DHCP snooping.

Displaying global DHCP snooping configuration information

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   show ip dhcp-snooping
   ```

Displaying VLAN DHCP snooping configuration information

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Displaying DHCP snooping port trust information

Procedure

1. Enter Ethernet Interface Configuration mode:

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

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

   ```
   show ip dhcp-snooping interface [<interface type>] [<port>]
   ```

Variable definitions

The following table describes the parameters for the **`show ip dhcp-snooping interface`** command.

Variable	Value
<interface type>	Specifies the type of interface
<port>	Specifies a port or list of ports.

Displaying the DHCP binding table

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Configuring DHCP Snooping Option 82 globally

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

The following table describes the parameters for the **`ip dhcp-snooping`** command.

Variable	Value
enable	Enables DHCP Snooping globally on the switch.
default	Configures DHCP Snooping on the switch to default values.
no	Disables DHCP Snooping globally on the switch.
option82	Enables DHCP Snooping with Option 82 globally on the switch.

Configuring VLAN-based DHCP Snooping Option 82

You must enable DHCP Snooping separately for each VLAN.

If DHCP Snooping is disabled on a VLAN, the switch forwards DHCP reply packets to all applicable ports, regardless of whether the port is trusted or untrusted.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Variable definitions

The following table describes the parameters for the **ip dhcp-snooping vlan** command.

Variable	Value
default	Configures DHCP Snooping on a VLAN to the default value. DEFAULT: disabled
no	Disables DHCP Snooping on a VLAN. If you do not specify a VLAN ID, DHCP Snooping is disabled on all VLANs.
option82	Enables DHCP Snooping with Option 82 on a VLAN.
vlanID	Specifies the ID of the preconfigured VLAN on which you want to enable DHCP Snooping. RANGE: 1 to 4094

Displaying DHCP Snooping

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   show ip dhcp-snooping
   ```

Example

The following figure provides an example output of the **show ip dhcp-snooping** command.

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

Displaying DHCP Snooping for an interface

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   show ip dhcp-snooping interface
   ```

Example

The following figure provides an example output of the **show ip dhcp-snooping interface** command.

```
Switch#show ip dhcp-snooping interface
       DHCP        ARP         Source        DHCP Snooping
Port Snooping   Inspection  Guard Mode  Option82 Subscriber Id
---- ---------  ----------  ----------  ----------------------
1    Untrusted  Untrusted   Disabled
2    Untrusted  Untrusted   Disabled
3    Untrusted  Untrusted   Disabled
4    Untrusted  Untrusted   Disabled
5    Untrusted  Untrusted   Disabled
6    Untrusted  Untrusted   Disabled
7    Untrusted  Untrusted   Disabled
8    Untrusted  Untrusted   Disabled
9    Untrusted  Untrusted   Disabled
10   Untrusted  Untrusted   Disabled
11   Untrusted  Untrusted   Disabled
12   Untrusted  Untrusted   Disabled
13   Untrusted  Untrusted   Disabled
14   Untrusted  Untrusted   Disabled
15   Untrusted  Untrusted   Disabled
16   Untrusted  Untrusted   Disabled
17   Untrusted  Untrusted   Disabled
18   Untrusted  Untrusted   Disabled
19   Untrusted  Untrusted   Disabled
----More (q=Quit, space/return=Continue)----
```

Configuring DHCP snooping using EDM

This section provides procedures to configure DHCP snooping using EDM.

Configuring DHCP snooping and Option 82 globally using EDM

Use this procedure to enable or disable global DHCP Snooping parameters for the switch.

Before you begin

- In Layer 3 mode, DHCP Snooping must be enabled on Layer 3 VLANs spanning toward DHCP servers.
- Enable DHCP Relay.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Snooping Globals** tab.

4. For DHCP Snooping, perform one of the following:
   - Select the **DhcpSnoopingEnabled** check box to enable DHCP snooping.
   - Clear the **DhcpSnoopingEnabled** check box to disable DHCP snooping.
5. For Option 82 for Snooping, perform one of the following:
   - Select the **DhcpSnoopingOption82Enabled** box.
   - Clear the **DhcpSnoopingOption82Enabled** box
6. On the toolbar, click **Apply**.

Configuring DHCP snooping and Option 82 on a VLAN using EDM

Use this procedure to enable or disable DHCP Snooping and DHCP Snooping with Option 82 parameters on the VLAN.

Before you begin

About this task

- Enable DHCP snooping separately for each VLAN ID.

Important:

If DHCP snooping is disabled on a VLAN, the switch forwards DHCP reply packets to all applicable ports, whether the port is trusted or untrusted.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Snooping-VLAN** tab.
4. To select a VLAN to edit, click the **VLAN ID**.
5. In the VLAN row, double-click the cell in the **DhcpSnoopingEnabled** column.
6. Select a value from the following List:
   - **true** to enable DHCP Snooping for the VLAN
   - **false** to disable DHCP Snooping for the VLAN
7. In the VLAN row, double-click the cell in the **VlanOption82Enabled** column.
8. Select one of the values from the following list:
   - **true** to enable DHCP Snooping with Option 82 for the VLAN
   - **false** to disable DHCP Snooping with Option 82 for the VLAN.
9. On the toolbar, click **Apply**.

DHCP Snooping-VLAN Tab Field Descriptions

Use the data in the following table to use the **DHCP Snooping-VLAN** tab.

Name	Description
VlanId	Identifies the VLANs configured on the switch.
DhcpSnoopingEnabled	Enables or disables DHCP snooping on a VLAN.
VlanOption82Enabled	Enables or disables DHCP Snooping Option 82 on a VLAN.

Configuring DHCP snooping port trust and DHCP Option 82 for a port using EDM

Use this procedure to configure DHCP Snooping on a port to configure port trust and to enable or disable DHCP Snooping with Option 82 for a port. Used with DHCP Snooping, DHCP Option 82 assists in tracking of end device locations.

Ports are untrusted by default.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. In the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Snooping-port** tab.
4. To select a port to edit, click a **Port** row.
5. In the port row, double-click the cell in the **DhcpSnoopingIfTrusted** column
6. Select a value from the following list:
   - trusted.
   - untrusted
7. Repeat the previous two steps for each port you want to configure.
8. Double-click the **DhcpSnoopingIfOption82SubscriberId** for a port.
9. Type a subscriber ID value for the port.
10. Repeat the previous two steps for each port you want to configure
11. On the toolbar, click **Apply**.

DHCP Snooping-port Tab Field Descriptions

Use the data in the following table to use the **DHCP Snooping-port** tab.

Name	Description
Port	Identifies the ports on the switch.
DhcpSnoopingIfTrusted	Specifies if the port is trusted or untrusted. Default is false.

Table continues…

Name	Description
DhcpSnoopingIfOption82Subscribed	Specifies the DHCP Option 82 subscriber ID for the port. The value is a character string from 1 to 64 characters.

Viewing the DHCP binding information using EDM

Use this procedure to view the current DHCP snooping binding table.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **DHCP Snooping**.
3. In the work area, click the **DHCP Bindings** tab.

DHCP Bindings Tab Field Descriptions

Use the data in the following table to use the **DHCP Bindings** tab.

Name	Description
VlanId	Identifies the VLAN on the switch.
MacAddress	Indicates the MAC address of the DHCP client.
AddressType	Indicates the MAC address type of the DHCP client.
Address	Indicates IP address of the DHCP client.
Interface	Indicates the interface to which the DHCP client is connected.
LeaseTime(sec)	Indicates the lease time (in seconds) of the DHCP client binding.
TimeToExpiry(sec)	Indicates the time (in seconds) before a DHCP client binding expires.
Source	Indicates the source of the binding table entry.

Chapter 13: 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 ARP Inspection is a security feature that validates ARP packets in the network.

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

The address binding table is dynamically built from information gathered in the DHCP request and reply when DHCP snooping is enabled. The MAC address from the DHCP request is paired with the IP address from the DHCP reply to create an entry in the DHCP binding table. For information about the DHCP binding table, see DHCP binding table on page 287.

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

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

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

Configuring Dynamic ARP Inspection using CLI

This section provides procedures to configure Dynamic ARP Inspection using CLI.

Displaying the ARP table

Procedure

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

   ```
   show arp-table
   ```

Example

The following figure provides a sample of the **`show arp-table`** command.

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

Configuring dynamic ARP inspection on a VLAN

Enable dynamic ARP inspection on a VLAN to validate ARP packets transmitted on that VLAN. You must enable dynamic ARP inspection separately for each VLAN as required. Dynamic ARP inspection is disabled by default.

Before you begin

- Enable DHCP snooping globally on the switch.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   [no] ip arp-inspection vlan <vlanID>
   ```

Variable definitions

The following table describes the parameters for the **`ip arp-inspection vlan`** command.

Variable	Value
<vlanID>	Specifies the VLAN in your network. Values range from 1 to 4094.

Configuring dynamic ARP inspection port trust

Configure dynamic ARP inspection port trust to specify whether a particular port or range of ports is trusted or untrusted. Ports are untrusted by default.

Procedure

1. Enter Interface Configuration mode:

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

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

   ```
   ip arp-inspection [port <LINE>] <trusted|untrusted>
   ```

Variable definitions

The following table describes the parameters for the **`ip arp-inspection`** command.

Variable	Value
port *<LINE>*	Specifies a port or list of ports.

Configuring dynamic ARP inspection port trust to default

Configure dynamic ARP inspection port trust to default to specify that a particular port, a range of ports, or all ports on the switch are untrusted.

Procedure

1. Enter Interface Configuration mode:

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

2. Configure dynamic ARP inspection port trust to default on a single port or list of ports by using the following command:

   ```
   default ip arp-inspection port <LINE>
   ```

3. Configure dynamic ARP inspection port trust to default on all ports on the switch by using the following command

   ```
   default ip arp-inspection port all
   ```

Variable definitions

The following table describes the parameters for the **default ip arp-inspection port** command.

Variable	Value
<LINE>	Specifies a port or list of ports.

Displaying VLAN dynamic ARP inspection configuration information

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

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

Displaying dynamic ARP inspection port trust information

Procedure

1. Enter Interface Configuration mode:

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

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

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

Variable definitions

The following table describes the parameters for the **show ip arp-inspection interface** command.

Variable	Value
<interface type>	Specifies the type of interface.
<port>	Specifies a port or list of ports.

Dynamic ARP Inspection using EDM

This section provides procedures to configure Dynamic ARP Inspection using EDM.

Configuring dynamic ARP inspection on a VLAN using EDM

Use this procedure to enable or disable dynamic ARP inspection on the VLAN.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **Dynamic ARP Inspection (DAI)**.
3. In the work area, click the **ARP Inspection-VLAN** tab.
4. In the **ArpInspectionEnabled** column, double-click the cell for the VLAN you want to configure.
5. From the list, select **true** to enable ARP inspection on the VLAN or select **false** to disable ARP inspection on the VLAN.
6. On the toolbar, click **Apply**.

ARP Inspection-VLAN Tab Field Descriptions

Use the data in the following table to use the **ARP Inspection-VLAN** tab.

Name	Description
VlanId	Identifies VLANs configured on the switch.
ARPInspectionEnabled	Enables or disables ARP inspection on a VLAN.

Configuring dynamic ARP inspection on a port using EDM

Use this procedure to enable or disable dynamic ARP inspection on a port.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **Dynamic ARP Inspection (DAI)**.
3. In the work area, click the **ARP Inspection-Port** tab.
4. In the **ArpInspectionIfTrusted** column, double-click the cell for the port you want to configure.
5. From the list, select **trusted** to enable ARP inspection on the port or select **untrusted** to disable ARP inspection on the port.
6. On the toolbar, click **Apply**.

ARP Inspection-port Tab Field Descriptions

Use the data in the following table to use the **ARP Inspection-port** tab.

Name	Description
Port	Identifies ports on the switch, using the unit/port format.
ARPInspectionIfTrusted	Configures a port as trusted or untrusted for ARP inspection.

Chapter 14: 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. It is a Layer 2, feature for each port that works closely with information in the Dynamic Host Control Protocol (DHCP) snooping Binding Table. For information about DHCP snooping, see DHCP snooping on page 286. When IP Source Guard is enabled on an untrusted port with DHCP snooping enabled, an IP filter entry is created or deleted for that port automatically, based on IP information stored in the corresponding DHCP snooping Binding Table entry. When a connecting client receives a valid IP address from the DHCP server, a filter is installed on the port to allow traffic only from the assigned IP address. A maximum of 10 IP addresses are allowed on each IP Source Guard-enabled port. When this number is reached, no additional filters are set up and traffic is dropped.

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

Important:

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

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

IP Source Guard configuration state	DHCP snooping configuration state	DHCP snooping Binding Entry action (untrusted ports)	IP Source Guard action
disabled or enabled	enabled	creates a binding entry	creates a filter for the IP address using the IP address from the Binding Table entry
enabled	enabled	creates a binding entry	creates a filter for the IP address using the IP address from the Binding Table entry

Table continues…

IP Source Guard configuration state	DHCP snooping configuration state	DHCP snooping Binding Entry action (untrusted ports)	IP Source Guard action
enabled	enabled	deletes 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

IP Source Guard does not support the following features:

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

You can configure IP Source Guard by using the Command Line Interface (CLI), Enterprise Device Manager (EDM) and SNMP.

Configuring IP Source Guard using CLI

This section provides procedures to configure IP Source Guard using CLI.

Before you begin

Before you can configure IP Source Guard, you must ensure the following:

- Dynamic Host Control Protocol (DHCP) snooping is globally enabled.
- The port is a member of a Virtual LAN (VLAN) configured with DHCP snooping and dynamic Address Resolution Protocol (ARP) Inspection.
- The bsSourceGuardConfigMode MIB object exists.

  This MIB object is used to control the IP Source Guard mode on an interface.

- the following applications are not enabled:
  - IP Fix
  - Baysecure

Note:

You can configure EAP and IP source guard simultaneously on the same port.

Important:

We recommend that you do not enable IP Source Guard on trunk ports. You can consume all hardware resources if IP Source Guard is enabled on trunk ports with a large number of VLANs that have DHCP snooping enabled and traffic sending can be interrupted for some clients.

Configuring IP Source Guard

Procedure

1. Enter Interface Configuration mode:

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

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

   ```
   [no] ip verify source interface {<interface type>] [<port>]}
   ```

Variable definitions

The following table describes the parameters for the **`ip verify source interface`** command.

Variable	Value
<interface type>	Specifies the interface type of the interface on which you want IP Source Guard enabled.
<port>	Specifies the interface type of the interface on which you want IP Source Guard enabled

Displaying IP Source Guard port configuration information

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show ip verify source [interface {<interface type>] [<port>]
   ```

Variable definitions

The following table describes the parameters for the **show ip verify source** command.

Variable	Value
<port>	Specifies the interface type of the interface on which you want IP Source Guard enabled.
<interface type>	Specifies the interface on which you want IP Source Guard enabled.

Displaying IP Guard-allowed addresses

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

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

   ```
   show ip source binding [<A.B.C.D>] [interface {[interface type>] [<port>]}]
   ```

Variable definitions

The following table describes the parameters for the **show ip source binding** command.

Variable	Value
<A.B.C.D>	Specifies the IP address or group of addresses that IP Source Guard allowed.
<port>	Specifies the interface type of the interface on which you want IP Source Guard enabled.
<interface type>	Specifies the type of interface for which you want IP Source Guard-allowed addresses displayed.

Configuring IP Source Guard using EDM

Use the procedures in this section to configure IP Source Guard to add a higher level of security to a port or ports by preventing IP spoofing.

Before you begin

- Globally enable Dynamic Host Control Protocol (DHCP) snooping.
- For information see Configuring DHCP snooping and Option 82 on a VLAN using EDM on page 294
- Ensure that the port is a member of a Virtual LAN (VLAN) configured with DHCP snooping and dynamic Address Resolution Protocol (ARP) Inspection.

- Confirm that the bsSourceGuardConfigMode MIB object exists.

  Use the MIB object to control the IP Source Guard mode on an interface.
- Ensure that the following applications are disabled:
  - IP Fix
  - Baysecure
  - Extensible Authentication Protocol over LAN (EAPOL)

Important:

We recommend that you do not enable IP Source Guard on trunk ports. You can consume all hardware resources if IP Source Guard is enabled on trunk ports with a large number of VLANs that have DHCP snooping enabled and traffic sending can be interrupted for some clients.

Configuring IP Source Guard on a port using EDM

Use this procedure to enable or disable a higher level of security on a port or ports.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree
2. From the Security tree, click **IP Source Guard (IPSG)**.
3. In the work area, click the **IP Source Guard-port** tab.
4. In the Mode column, double-click the cell of the port you want to configure.
5. Perform one of the following:
   - From the list, select **ip** to enable IP Source Guard
   - From the list, select **disabled** to disable IP Source Guard on the port.
6. On the toolbar, click **Apply**.

IP Source Guard-Port Tab Field Descriptions

Use the data in the following table to use the **IP Source Guard-Port** tab.

Name	Description
Port	Identifies the port number.
Mode	Identifies the Source Guard mode for the port. The mode can be disabled or ip. The default mode is disabled.

Filtering IP Source Guard addresses using EDM

Use this procedure to display IP Source Guard information for specific IP addresses.

Procedure

1. From the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **IP Source Guard (IPSG)**.
3. In the work area, click the **IP Source Guard-addresses** tab.
4. On the tool bar, click **Filter**.
5. In the IP Source Guard-addresses - Filter dialog, select the required parameters to display specific port IP Source Guard information.
6. Click **Filter**.

IP Source Guard-addresses Filter Dialog Field Descriptions

Use the data in the following table to use the **IP Source Guard-addresses Filter dialog**.

Name	Description
Condition	Defines the search condition. • **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. • **Contains** • **Does not contain** • Equals to
All records	Displays all entries in the table.

Chapter 15: 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 fundamentals

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

A defined action is reversed, or ceases, when the traffic rate in pps falls below the low-watermark setting. When an action of ‘drop’ is used, traffic is dropped when traffic exceeds the high-watermark and will not resume forwarding until the traffic rate falls below the low-watermark. When the action of ‘shutdown’ is used, the switch port is administratively shutdown when traffic exceeds the high-watermark and requires administrator intervention to re-enable the switch port to resume traffic forwarding.

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

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

Configuring Storm Control using CLI

This section provides procedures to configure Storm Control using CLI.

Configuring storm control

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   [no] storm-control [broadcast | multicast | unicast | all] [action
   [none | drop | shutdown ]] [enable] [high-watermark <10-100000000>]
   [low-watermark <10-100000000>] [poll-interval <5-300>] [trap-
   interval <0-1000]
   ```

Variable definitions

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

Variable	Description
action	Specifies the storm control action: • **drop**: Set storm control action to drop • **none**: • **shutdown**: Set storm control action to shutdown
high-watermark <10-100000000>	Specifies the high-watermark value in packets per second (pps). Range: 10 to 100000000 Default: 1000
low-watermark <10-100000000>	Specifies the low-watermark value in packets per second (pps). Range: 10 to 100000000 Default: 100
poll-interval <5-300>	Specifies the interval for watermark checking; the value varies in seconds. Range: 5 to 300 Default: 5
trap-interval <0-1000>	Specifies the interval for sending traps when the poll-intervals exceed. Range: 0 to 1000

Table continues…

Variable	Description
	Note: Value 0 means disabled (high watermark traps does not repeat). Default: 0

Displaying global storm control state

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

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

   ```
   show storm-control [broadcast | multicast | unicast | all]
   ```

Example

The following is a sample output of the **`show storm-control all`** command.

```
Switch(config)#show storm-control all
Storm Control Status    High Wm     Low Wm     Poll    Action      Trap
--------------------    --------    --------   -----   ---------   ----
Unicast     Disabled     1000        100        5       none        0
Broadcast   Disabled     1000        100        5       none        0
Multicast   Disabled     1000        100        5       none        0
```

Configuring Storm Control using EDM

This section provides procedures to configure Storm Control globally and for specific traffic type using EDM.

Configuring Storm Control globally

About this task

Use the following procedure to globally configure Storm Control using EDM

Procedure

1. In the navigation tree, double-click **Edit** to open the Edit tree.
2. In the Edit tree double-click **Storm Control**.
3. In the work area, click the **Globals** tab.

4. Configure the Storm Control parameters as required.
5. On the toolbar, click **Apply**.

Global Storm Control Field Descriptions

Use the following fields to configure Storm Control globally using EDM.

Name	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
HighWatermark(pps)	Indicates the high-watermark value for the port in packets per second (pps). RANGE: 10 to 100000000
PollInterval(secs)	Indicates the interval for watermark checking, the value varies in seconds. RANGE: 5 to 300
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)
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, double-click **Storm Control**.
3. In the work area click the **Broadcast** tab.
4. To select a port to configure, click the port **Index**.
5. In the port row, double-click the cell in the **Enabled** column.
6. Set a value from the drop-down list — **true** to enable Storm Control, or **false** to disable Storm Control for the specified port.
7. In the port row, double-click the cell in the **LowWatermark(pps)** column, and enter a value in the range `<10–100000000>`.
8. In the port row, double-click the cell in the **HighWatermark(pps)** column, and enter a value in the range `<10–100000000>`.
9. In the port row, double-click the cell in the **PollInterval(secs)**column, and enter a value in the range `<5–300>`.
10. In the port row, double-click the cell in the **TrapInterval**column, and enter a value in the range `<0–1000>`.
11. In the port row, double-click the cell in the **ActionType** column.
12. Set a value from the drop-down list — **none** to take no action, **drop** , or **shutdown** to shutdown Storm Control for specified port.
13. Click **Apply Selection**.
14. On the toolbar, click **Apply**.

Broadcast Storm Control Field Descriptions

The following table describes the fields associated with configuration of **Broadcast Storm Control** settings.

Name	Description
Index	Indicates the port number.
Enabled	Indicates the current setting for the port. Values include: • **true**: enables Storm Control on the port

Table continues…

Name	Description
	• **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
HighWatermark(pps)	Indicates the high-watermark value for the port in packets per second (pps). RANGE: 10 to 100000000
PollInterval(secs)	Indicates the interval for watermark checking, the value varies in seconds. RANGE: 5 to 300
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)
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, double-click **Storm Control**.
3. In the work area click the **Multicast** tab.
4. To select a port to configure, click the port **Index**.
5. In the port row, double-click the cell in the **Enabled** column.
6. Set a value from the drop-down list — **true** to enable Storm Control, or **false** to disable Storm Control for the specified port.

7. In the port row, double-click the cell in the **LowWatermark(pps)** column, and enter a value in the range <10–100000000>.
8. In the port row, double-click the cell in the **HighWatermark(pps)** column, and enter a value in the range <10–100000000>.
9. In the port row, double-click the cell in the **PollInterval(secs)column**, and enter a value in the range <5–300>.
10. In the port row, double-click the cell in the **TrapIntervalcolumn**, and enter a value in the range <0–1000>.
11. In the port row, double-click the cell in the **ActionType** column.
12. Set a value from the drop-down list — **none** to take no action, **drop** , or **shutdown** to shutdown Storm Control for specified port.
13. Click **Apply Selection**.
14. On the toolbar, click **Apply**.

Multicast Storm Control Field Descriptions

The following table describes the fields associated with configuration of the Multicast Storm Control setting.

Name	Description
Index	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
Enabled	Indicates the current setting for the port. Values include: • **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
HighWatermark(pps)	Indicates the high-watermark value for the port in packets per second (pps). RANGE: 10 to 100000000
PollInterval(secs)	Indicates the interval for watermark checking, the value varies in seconds. RANGE: 5 to 300
TrapInterval	Indicates the interval for sending traps when the poll-intervals exceed. RANGE: 0 to 1000

Table continues…

Name	Description
	Note: Value 0 means disabled (high watermark traps will not be repeated)
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, double-click **Storm Control**.
3. In the work area click the **Unicast** tab.
4. To select a port to configure, click the port **Index**.
5. In the port row, double-click the cell in the **Enabled** column.
6. Set a value from the drop-down list — **true** to enable Storm Control, or **false** to disable Storm Control for the specified port.
7. In the port row, double-click the cell in the **LowWatermark(pps)** column, and enter a value in the range `<10-100000000>`.
8. In the port row, double-click the cell in the **HighWatermark(pps)** column, and enter a value in the range `<10-100000000>`.
9. In the port row, double-click the cell in the **PollInterval(secs)** column, and enter a value in the range `<5-300>`.
10. In the port row, double-click the cell in the **TrapIntervalcolumn**, and enter a value in the range `<0-1000>`.
11. In the port row, double-click the cell in the **ActionType** column.
12. Set a value from the drop-down list — **none** to take no action, **drop** , or **shutdown** to shutdown Storm Control for specified port.
13. Click **Apply Selection**.
14. On the toolbar, click **Apply**.

Unicast Storm Control Field Descriptions

The following table describes the fields associated with configuration of the Unicast Storm Control settings.

Name	Description
Index	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
Enabled	Indicates the current setting for the port. Values include: • **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
HighWatermark(pps)	Indicates the high-watermark value for the port in packets per second (pps). RANGE: 10 to 100000000
PollInterval(secs)	Indicates the interval for watermark checking, the value varies in seconds. RANGE: 5 to 300
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)
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.

Unicast Storm Control Field Descriptions

The following table describes the fields associated with configuration of the Unicast Storm Control settings.

Name	Description
Index	Indicates the unique identifier allocated to an Aggregator by the local system. This is a read-only cell.
Enabled	Indicates the current setting for the port. Values include: • **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
HighWatermark(pps)	Indicates the high-watermark value for the port in packets per second (pps). RANGE: 10 to 100000000
PollInterval(secs)	Indicates the interval for watermark checking, the value varies in seconds. RANGE: 5 to 300
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)
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 16: Rate Limiting

This chapter provides conceptual information and procedures to configure Rate limiting using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

Rate limiting

The Rate Limiting feature lets you configure the threshold limits for broadcast and multicast packets ingressing on a port for a given time interval. The switch drops packets received above the threshold value if the traffic ingressing on the port exceeds the threshold. The hardware restrictions on this platform do not allow you to determine if the traffic from a port is the cause of excess broadcast or multicast traffic. Consequently you cannot perform port-specific actions such as disabling a port. You can generate a trap to detect the excess traffic or you can configure the switch to store a message in the system log when the traffic on the port exceeds the threshold value. This message in the system log conveys that some traffic to the switch is dropped.

When the volume of either packet type is high, placing severe strain on the network (often referred to as a "storm"), you can set the forwarding rate of those packet types to not exceed a specified percentage of the total available bandwidth. The pps (Packets Per Second) value you set is a small amount of the maximum value of pps for the maximum available bandwidth that is 262143 pps.

Important:

All Rate Limiting configuration settings are applied across the entire unit. You cannot set some ports in the unit to limit broadcast traffic with a value of X pps and some other ports in the same to limit multicast traffic with a value of Y pps.

You can view the rate limiting configuration settings and statistics with the **`show rate-limit`** command or the **`show running-config`** CLI command. You can also limit the percentage of multicast traffic, or broadcast traffic, or both with **`rate-limit`** CLI command.

Note:

Storm Control and Rate Limiting are disabled by default. Only one of these features can be enabled at any one time. In order to use Rate Limiting, you must ensure that Storm Control is globally disabled.

Configuring Rate Limiting using CLI

This section provides procedures to configure Rate Limiting using CLI.

Configuring rate limiting

Configure rate limiting in packets per second for the specified traffic type: either multicast, broadcast, or both.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   [no] [default] rate-limit [multicast|broadcast|both] <0-262143>
   ```

Variable definitions

The following table describes the parameters for the **`rate-limit`** command.

Variable	Value
multicast |broadcast | both	Applies rate limiting, in packets/second, to the specified type of traffic: • multicast — applies rate limiting to multicast packets • broadcast — applies rate limiting to broadcast packets • both — applies rate limiting to both multicast and broadcast packets
<0–262143>	Sets the pps (Packets Per Second) upper threshold limit for the traffic type. When the volume of packets exceeds this threshold, packets are dropped. The pps value you set is a small percent of the maximum value of pps for the total available bandwidth (262143 pps).
no	Disables rate limiting on the switch or stack
default	Restores the default value for rate limiting for the switch or stack

Displaying rate limit configuration

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show rate-limit
   ```

Example

The following figure displays sample output from the **`show rate-limit`** command.

```
Switch#show rate-limit
Packet Type     Limit
-----------     -----
Both            0 pps
```

Configuring Rate Limiting using EDM

This section provides procedures to configure Rate Limiting using EDM.

Configuring rate limiting using EDM

Use this procedure to display and configure rate limiting on a switch.

Procedure

1. From the Device Physical View, click a unit.
2. From the navigation tree, click **Edit**.
3. In the Edit tree, click **Unit**.
4. In the work area, select the **Rate Limit** tab.
5. To a rate limit, click a TrafficType row.
6. Double-click the cell in the **AllowedRatePps** column.
7. Type a value.
8. Double-click the cell in the **Enable** column.
9. Select a value from the list — true to enable the traffic type, or false to disable the traffic type.
10. On the toolbar, click **Apply**.

Rate Limit Tab Field Descriptions

Use the data in the following table to use the **Rate Limit** tab.

Name	Description
Traffic Type	Specifies the traffic type.
AllowedRatePps	Allowed traffic rate packets/second. It is in the range of 0–262143. **Important:** Rate Limiting feature is disabled when AllowedRatePps is set to 0.
Enable	When Enable is set to True, the TrafficType can either be multicast, broadcast, or both. **Important:** You cannot set the Enabled field for both multicast and broadcast TrafficType to False at the same time. This is an illegal configuration.

Chapter 17: 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+

TACACS+ is a security application implemented as a client/server-based protocol that provides centralized validation of users attempting to gain access to a router or network access server.

TACACS+ differs from RADIUS in two important ways:

- TACACS+ is a TCP-based protocol.
- TACACS+ uses full packet encryption, rather than only encrypting the password (RADIUS authentication request).

Important:

TACACS+ encrypts the entire body of the packet but uses a standard TACACS+ header.

TACACS+ separates authentication, authorization, and accounting services.

This means that you can selectively implement one or more TACACS+ service. TACACS+ provides management of users who access the switch through Telnet, serial, and SSH v2 connections. TACACS+ supports users only on CLI.

Access to the WEB interface and SNMP are disabled when TACACS+ is enabled.

The TACACS+ protocol is a draft standard available at https://datatracker.ietf.org/doc/draft-ietf-opsawg-tacacshttps://datatracker.ietf.org/drafts/draftgrant-%20tacacs/

Important:

TACACS+ is not compatible with previous versions of TACACS.

TACACS+ architecture

You can configure TACACS+ by using the following methods:

- Connect the TACACS+ server through a local interface. Management PCs can reside on an out-of-band management port or serial port, or on the corporate network. The TACACS + server is placed on the corporate network so that it can be routed to the switch.
- Connect the TACACS+ server through the management interface by using an out-of-band management network.

You can configure a secondary TACACS+ server for backup authentication. You specify the primary authentication server when you configure the switch for TACACS+.

Feature operation

During the logon process, the TACACS+ client initiates the TACACS+ authentication session with the server. After successful authentication, if TACACS+ authorization is enabled, the TACACS+ client initiates the TACACS+ authorization session with the server. After successful authentication, if TACACS+ accounting is enabled, the TACACS+ client sends accounting information to the TACACS + server.

TACACS+ authentication

TACACS+ authentication offers complete control of authentication through logon and password dialog and response. The authentication session provides user name and password functionality.

You cannot enable both RADIUS and TACACS+ authentication on the same interface. However, you can enable RADIUS and TACACS+ on various interfaces; for example, RADIUS on the serial connection and TACACS+ on the Telnet connection.

Note:

Prompts for logon and password occur prior to the authentication process. If TACACS+ fails because no valid servers are available, the user name and password are used for the local database. If TACACS+ or the local database return an access denied packet, the authentication process stops. No other authentication methods are attempted.

TACACS+ authorization

The transition from TACACS+ authentication to the authorization phase is transparent to the user. Upon successful completion of the authentication session, an authorization session starts with the authenticated user name. The authorization session provides access-level functionality.

With TACACS+ authorization, you can limit the switch commands available to a user. When TACACS+ authorization is enabled, the NAS uses information retrieved from the user profile, which is either in the local user database or on the security server, to configure the user session. The user is granted access to a requested command only if the information in the user profile allows it.

TACACS+ authorization is not mandatory for all privilege levels.

When authorization is requested by the NAS, the entire command is sent to the TACACS+ daemon for authorization. You preconfigure command authorization on the TACACS+ server by specifying a list of regular expressions that match command arguments and associating each command with an action to deny or permit. For an example of the configuration required on the TACACS+ server, see TACACS+ server configuration example on page 326.

Authorization is recursive over groups. If you place a user in a group, the daemon looks in the group for authorization parameters if it cannot find them in the user declaration.

If authorization is enabled for a privilege level to which a user is assigned, the TACACS+ server denies commands for which access is not explicitly granted for the specific user or for the user group. On the daemon, ensure that each group is authorized to access basic commands such as `enable` or `logout`.

If the TACACS+ server is not available or an error occurs during the authorization process, the only command available is `logout`.

In the TACACS+ server configuration, if no privilege level is defined for a user but the user is allowed to execute at least one command, the user defaults to privilege level 0. If all commands are explicitly denied for a user, the user cannot access the switch at all.

Changing privilege levels at run time

You can change privilege levels at run time. To change privilege levels at run time, use the following command:

```
tacacs switch level [<level>]
```

[<level>] is the privilege level you want to access.

Note:

You are prompted to provide the required password. If you do not specify a level in the command, the administration level (15) is selected by default.

To return to the original privilege level, enter the following command: `tacacs switch back`

To support run time switching of users to a particular privilege level, you must preconfigure a dummy user for that level on the daemon. The format of the user name for the dummy user is $enab<n>$ where <n> is the privilege level to which you want to allow access.

For an example of the configuration required on the TACACS+ server, see TACACS+ server configuration example on page 326.

TACACS+ server configuration example

The following example shows a configuration sample for a Linux TACACS+ 4.0.4 server.

```
#Set the server key. You must configure an identical key on the switches communicating
with the TACACS+ server.

key = bayproject

#Set the accounting file on the server. All accounting records are written as text to
this filename.

accounting file = /usr/local/var/log/tac_plus.act

# You can configure user authentication separately for PAP, ARAP, CHAP, and normal
logins. You can also configure a global authentication method to be used if a per-
protocol method is not specified.
# You cannot use a global user password for outbound PAP.
# The following example assigns to a user four different passwords for inbound and
outbound:
# user = user1 {
#        chap = cleartext "chap_password"
#        pap = cleartext "inbound_pap_password"
#        opap = cleartext "outbound_pap_password"
#        login = des XQj4892fjk
#        }

# You can set the default authentication to use a passwd(5) file. With this option, when
a user does not appear in the configuration file, the daemon attempts to authenticate the
user using passwords from this file.
# default authentication = file /etc/passwd

# Configure groups:

group = vlan {
  login = cleartext vlan

# Specify the permitted commands:


  cmd = enable { permit .* }
  cmd = configure { permit .* }
  cmd = vlan { permit .* }
  cmd = show { permit .* }
  cmd = exit { permit .* }
  cmd = logout { permit .* }
  cmd = tacacs { permit .* }
}

group = trunk {
  login = cleartext trunk
  cmd = enable { permit .* }
  cmd = configure { permit terminal }
  cmd = mlt { permit .* }
  cmd = show { permit .* }
  cmd = exit { permit .* }
  cmd = logout { permit .* }
  cmd = tacacs { permit .* }
}

group = mirror {
  login = cleartext mirror
```

```
  cmd = enable { permit .* }
  cmd = configure { permit terminal }
  cmd = port-mirroring { permit .* }
  cmd = show { permit .* }
  cmd = exit { permit .* }
  cmd = logout { permit .* }
  cmd = tacacs { permit .* }
}

group = ipmgr {
  login = cleartext ipmgr
  cmd = enable { permit .* }
  cmd = configure { permit terminal }
  cmd = ipmgr { permit .* }
  cmd = show { permit .* }
  cmd = exit { permit .* }
  cmd = logout { permit .* }
  cmd = tacacs { permit .* }
}

# Configure the user accounts and assign the users to groups:


user = vlan1 {


  member = vlan # assigns the user vlan1 to the vlan group
  service = exec {
  priv-lvl = 0 # the CLI level displayed on switch
  }
}

user = trunk1 {
  member = trunk
  service = exec {
    priv-lvl = 1
  }
}

user = mirror1 {
  member = mirror
  service = exec {
    priv-lvl = 2
  }
}

user = ipmgr1 {
  member = ipmgr
  service = exec {
    priv-lvl = 3
  }
}

# You can configure an expiry date for a user password. Starting on the expiry date, the
user password becomes invalid. A warning message is sent to the user prior to the
expiration date.
# The 'expires' field in the configuration file is not consulted if passwd(5) files are
used for authentication. In this case, the 'shell' field of the password file is checked
for the expiry date.

#user = user2 {
#    expires = "MMM DD YYYY"
#    password = cleartext "user2_pass"
#}
```

```
# To check the configuration file syntax, use the tac_plus -P -C command. Any error
messages will be displayed on the terminal.
```

TACACS+ accounting

TACACS+ accounting enables you to track the following items:

- the services accessed by users
- the amount of network resources consumed by users

When you enable accounting, the NAS reports user activity to the TACACS+ server in the form of accounting records. Each accounting record contains accounting attribute=value (AV) pairs. The accounting records are stored on the security server. You can analyze the accounting data for network management and auditing.

TACACS+ accounting provides information about user CLI terminal sessions within serial, Telnet, or SSH shells (from CLI management interface).

The accounting record includes the following information:

- user name
- date
- start, stop, or elapsed time
- access server IP address
- reason

You cannot customize the set of events that TACACS+ accounting monitors and logs. TACACS + accounting logs the following events:

- user logon and logoff
- logoff generated because of activity timeout
- unauthorized command
- Telnet/SSHv2 session closed (not logged off)

Feature limitations

The following features are not supported in the current implementation of TACACS+:

- S/KEY (One Time Password) authentication.
- PPP/PAP/CHAP/MSCHAP authentication methods.
- The FOLLOW response of a TACACS+ server, in which the authentication, authorization, and accounting (AAA) services are redirected to another server. The response is interpreted as an authentication failure.

- User capability to change passwords at run time over the network. The system administrator must change user passwords locally on the server.

Configuring TACACS+ using CLI

This section provides procedures to configure TACACS+ using CLI to perform AAA services for system users.

Configuring switch TACACS+ server settings

Before you begin

- Configure the TACACS+ server to add to your system.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   tacacs server {[host <A.B.C.D> | key <key> | port <1-65535> |
   secondary-host <A.B.C.D> ]}
   ```

Variable definitions

The following table describes the parameters for the **`tacacs server`** command.

Variable	Value
host <*A.B.C.D*>	Specifies the IP address of the primary server to add or configure.
key <*key*>	Specifies the secret authentication and encryption key used for all communications between the NAS and the TACACS+ server. The key, also referred to as the shared secret, must be the same as the one defined on the server. You are prompted to confirm the key when you enter it. **Note:** The key parameter is a required parameter when you create a new server entry. The parameter is optional when you modify an existing entry.

Table continues…

Variable	Value
port *<1–65535>*	Specifies the TCP port for TACACS+. DEFAULT: 49
secondary-host *<A.B.C.D>*	Specifies the IP address of the secondary server. The secondary server is used only if the primary server does not respond.

Disabling switch TACACS+ server settings

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   no tacacs server
   ```

   OR

   ```
   default tacacs server
   ```

   These commands erase settings for the TACACS+ primary and secondary servers, secret key, and restore default port settings.

Enabling remote TACACS+ services

Use the following procedure to enable remote TACACS+ services to provide services to remote users over serial or Telnet/SSH connections.

Before you begin

- Configure a TACACS+ server on the switch before you enable remote TACACS+ services.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To enable remote TACACS+ services for serial connections, enter the following command:

   ```
   cli password serial tacacs
   ```

3. To enable remote TACACS+ services for Telnet connections, enter the following command:

   ```
   cli password telnet tacacs
   ```

Enabling or disabling TACACS+ authorization

TACACS+ authorization is disabled by default.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To enable TACACS+ authorization, enter the following command:

   ```
   tacacs authorization enable
   ```

3. To disable TACACS+ authorization, enter the following command:

   ```
   tacacs authorization disable
   ```

Configuring TACACS+ authorization privilege levels

Use the following procedure to configure TACACS+ authorization privilege levels to specify the privilege levels to which TACACS+ authorization applies.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   tacacs authorization level { ALL | <LINE> | NONE }
   ```

Variable definitions

The following table describes the parameters for the **`tacacs authorization level`** command.

Variable	Value
ALL	Enables authorization for all privilege levels.
LINE	Enables authorization for a specific privilege level. LINE is a numerical value or a list of numerical values in the range of 0 to 15.
NONE	Authorization is not enabled for any privilege level. All users can execute any command available on the switch. The default authorization level is NONE.

Enabling or disabling TACACS+ accounting

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To enable TACACS+ accounting, enter the following command:

   ```
   tacacs accounting enable
   ```

3. To disable TACACS+ accounting, enter the following command:

   ```
   tacacs accounting disable
   ```

Configuring the switch TACACS+ level

Use the following procedure to configure the switch TACACS+ level to select a new level for a switch or use the last configured level.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. To configure a new TACACS+ level for a switch, enter the following command:

   ```
   tacacs switch level <1-15>
   ```

   If no level is specified, the switch TACACS+ level defaults to 15.

3. To use the last configured TACACS+ level for a switch, enter the following command:

   ```
   tacacs switch back
   ```

Viewing TACACS+ information

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show tacacs
   ```

Configuring TACACS using EDM

This section provides procedures to configure TACACS+ using EDM to perform AAA services for system users.

Enabling or disabling TACACS+ accounting using EDM

Use this procedure to enable or disable TACACS+ accounting using EDM.

Procedure

1. In the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **TACACS+**
3. In the work area, click the **Globals** tab.
4. Perform one of the following:
   - To enable accounting, select the **Accounting** checkbox.
   - To disable accounting, deselect the **Accounting** checkbox.
5. On the toolbar, click **Apply**.

Globals Tab Field Descriptions

Use the data in the following table to use the **Globals** tab.

Name	Description
Accounting	Enables or disables accounting: • Select the checkbox to enable accounting • Deselect the checkbox to disable accounting

Enabling or disabling TACACS+ authorization using EDM

Use this procedure to enable or disable TACACS+ accounting using EDM.

Procedure

1. In the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **TACACS+**
3. In the work area, click the **Globals** tab.
4. Perform one of the following:
   - To enable authorization, select the **AuthorizationEnabled** checkbox .
   - To disable authorization, deselect the **AuthorizationEnabled** checkbox.

5. On the toolbar, click **Apply**.

Globals Tab Field Descriptions

Use the data in the following table to use the **Globals** tab.

Name	Description
AuthorizationEnabled	Enable or disable the authorization feature.

Configuring the switch TACACS+ levels using EDM

Use this procedure to configure the switch TACACS+ levels using EDM.

Procedure

1. In the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **TACACS+**
3. In the work area, click the **Globals** tab.
4. In the **AuthorizationLevels** field, click the level of authorization <0-15>.
5. On the toolbar, click **Apply**.

Globals Tab Field Descriptions

Use the data in the following table to use the **Globals** tab.

Name	Description
AuthorizationLevels <0–15>	This object controls which CLI command privilege levels will be authorized by TACACS+.

Creating a TACACS+ server using EDM

Use this procedure to create a TACACS+ server.

Procedure

1. In the navigation tree, double-click **Security** to open the Security tree.
2. From the Security tree, click **TACACS+**.
3. In the work area, click the **TACACS+ Server** tab.
4. On the toolbar, click **Insert** to open the Insert TACACS+ Server dialog.
5. In the **Address** field, enter the IP address of the TACACS+ server.
6. In the **PortNumber** field, enter the TCP port on which the client establishes a connection to the server.

7. In the **Key** field, enter the secret key shared with this TACACS+ server.
8. In the **Confirm Key** field, reenter the secret key shared with this TACACS+ server.
9. In the **Priority** field, click **Primary** or **Secondary** to determine the order in which the TACACS+ server is used.
10. Click **Insert** to accept the change and return to the work area.

TACACS+ Server Tab Field Descriptions

Use the data in the following table to use the **TACACS+ Server** tab.

Name	Description
AddressType	Specifies the type of IP address used on the TACACS+ server.
Address	The IP address of the TACACS+ server referred to in this table entry.
PortNumber	The TCP port on which the client establishes a connection to the server. A value of 0 indicates that the system specified default value is used.
Key	Secret key to be shared with this TACACS+ server.
Priority	Determines the order in which the TACACS+ servers will be used. If more than one server shares the same priority, they will be used in lexicographic order (the order of entries in this table).

Chapter 18: Configuration examples

TACACS+ server configuration examples

This section describes basic configuration examples of the TACACS+ server.

Extreme Networks Identity Engine Ignition Server TACACS+ Configuration Example

The following section shows the steps required to configure TACACS+ on Extreme Networks Identity Engines Ignition Server, Release 8.0. Use the preceding information to configure the switch.

A TACACS+ server responds to and audits network access requests. In an installation, the Identity Engines Ignition Server is the TACACS+ server.

The example displays how to do the following:

- Enable TACACS+
- Configure a user
- Create a command set
- Configure the authentication protocol policy
- Create the authorization policy
- Configure TACACS+ authenticators

For more information on the Ignition Server, see 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.

SNMP MIB support

The SNMP agent with industry standard Management Information Bases (MIB) and private MIB extensions ensures ompatibility with existing network management tools.

The IETF standard MIBs supported on the switch include MIB-II (originally published as RFC 1213, then split into separate MIBs as described in RFCs 4293, 4022, and 4113), Bridge MIB (RFC 4188), and the RMON MIB (RFC 2819), which provides access to detailed management statistics.

With SNMP management, you can configure SNMP traps (on individual ports) to generate automatically for conditions such as an unauthorized access attempt or changes in the operating status of a port.

Table 4: SNMP MIB support

Application	Standard MIBs	Proprietary MIBs
S5 Chassis MIB		s5cha127.mib
S5Agent MIB		s5age140.mib
RMON	rfc1757.mib	
MLT		rcMLT
SNMPv3 MIBs	RFCs 2571, 2572, 2573, 2574, 2575, 2576	
MIB2	rfc1213.mib	
IF-MIB	rfc2233.mib	
Etherlike MIB	rfc1643.mib	
Interface Extension MIB		s5ifx100.mib
Switch Bay Secure		s5sbs102.mib
System Log MIB		bnlog.mib
S5 Autotopology MIB		s5emt104.mib
VLAN		rcVlan
Entity MIB	RFC 2037	
Spanning Tree	RFC1493 Bridge MIB	
LLDP-MIB	IEEE 802.1ab	

Management Agent

The SNMP agent is trilingual and supports exchanges by using SNMPv1, SNMPv2c, and SNMPv3. SNMPv1 communities provide support for SNMPv2c by introducing standards-based GetBulk

retrieval capability. SNMPv3 support provides MD5 and SHA-based user authentication and message security as well as DES-based message encryption.

Modules that support MIB are:

Standard MIBs

- MIB II (RFC 1213)
- Bridge MIB (RFC 1493) and proposed VLAN extensions
- 802.1Q Bridge MIB
- 802.1p
- Ethernet MIB (RFC 1643)
- RMON MIB (RFC 1757)
- SMON MIB
- High Capacity RMON
- Interface MIB (RFC2233)
- Entity MIB (RFC2037)
- SNMPv3 MIBs (RFC 2271 –RFC 2275)

Proprietary MIBs

- s5Chassis MIB
- s5Agent MIB
- Interface Extension MIB
- s5 Multi-segment topology MIB
- s5 Switch BaySecure MIB
- System Log MIB
- RapidCity Enterprise MIB
- rcDiag (Conversation steering) MIB
- rcVLAN MIB
- rcMLT MIB

SNMP trap support

The SNMP agent with industry standard SNMPv1 traps and private SNMPv1 trap extensions are supported.

Trap name	MIB	Sent when
lldpRemTablesChange	LLDP-MIB	Changes in lldpStatsRemTableLastChangeTime occur.
risingAlarm	s5CtrMIB	A rising alarm is fired.
fallingAlarm	s5CtrMIB	A falling alarm is fired.
pethPsePortOnOffNotification	rfc3621MIB	Pse Port is delivering or is not delivering power to the PD.
pethMainPowerUsageOnNotification	rfc3621MIB	The usage power is above the threshold.
pethMainPowerUsageOffNotification	rfc3621MIB	The usage power is below the threshold.
entConfigChange	rfc4133MIB	A change in either of these tables occurred: entPhysicalTable, entLogicalTable, entLPMappingTable, entAliasMappingTable.
coldStart	rfc3418MIB	The system is powered on.
warmStart	rfc3418MIB	The system restarts due to a management reset.
linkDown	rfc2863MIB	The link state changes to down on a port.
linkUp	rfc2863MIB	The link state changes to up on a port.
authenticationFailure	rfc3418MIB	SNMP authentication failure occurs.
lldpXMedTopologyChangeDetected	lldpExtMedMIB	A new remote device is attached to a local port, or a remote device is disconnected.
bsAdacPortConfigNotification	bayStackAdacMIB	The maximum number of devices supported per port is reached.
bsDhcpSnoopingBindingTableFull	bayStackDhcpSnoopi ngMIB	An attempt is made to add a new DHCP binding entry when the binding table is full.
bsDhcpSnoopingTrap	bayStackDhcpSnoopi ngMIB	A DHCP packet is dropped.
bsaiArpPacketDroppedOnUntrustedPort	bayStackArpInspectio nMIB	An ARP packet is dropped on an untrusted port due to an invalid IP/MAC binding.
bsSourceGuardReachedMaxIpEntries	bayStackSourceGuar dMIB	The maximum number of IP entries on a port has been reached.

Table continues…

Trap name	MIB	Sent when
bsSourceGuardCannotEnablePort	bayStackSourceGuar dMIB	There are insufficient resources available to enable IP source guard checking on a port.
rcnBpduReceived	rcTrapsMIB	A BPDU is received on a port which has BPDU filtering enabled.
bsnConfigurationSavedToNvram	bsnMIB	All switch configuration is saved to NVRAM.
bsnEapAccessViolation	bsnMIB	An EAP access violation occurs.
bsnLacTrunkUnavailable	bsnMIB	An attempt is made to form an 802.3ad LAG trunk, but there are no available resources to create a new trunk.
bsnLoginFailure	bsnMIB	An attempt to login to the system fails as a result of an incorrect password.
bsnLacPortDisabledDueToLossOfVLACPDU	bsnMIB	A port is disabled due to the loss of a VLACP PDU.
bsnLacPortEnabledDueToReceiptOfVLACPDU	bsnMIB	A port is enabled due to receipt of a VLACP PDU.
bsnEapRAVError	bsnMIB	An Eap client MAC address was authorized on a port, but the port could not be moved to the Radius-Assigned VLAN.
s5EtrNewSbsMacAccessViolation	s5CtrMIB	A MAC address violation is detected.
s5CtrFanDirectionError	s5CtrMIB	A fan component's direction is incorrect
s5CtrHighTemperatureError	s5CtrMIB	The system is overheated.

Sticky MAC address configuration examples

The following configuration examples describe the basic steps required to:

- configure a device to learn sticky MAC addresses on a range of ports
- manually configure sticky MAC address on an individual port

Note:

Extreme Networks recommends that you disable autosave when sticky mac is enabled.

Before you begin

Globally enable the following:

- MAC security
- autolearning mode

For the specific interfaces on which you are configuring sticky MAC address, enable the following :

- MAC security
- autolearning sticky mode

Configuring a device to learn sticky MAC addresses on a range of ports:

Ports 1/6 through 1/14 are used for this example.

1. Enable MAC security and auto-learning globally.

```
Switch(config)#mac-security auto-learning sticky
Extreme Networks recommends disabling autosave when sticky mac is enabled
Switch(config)#mac-security enable
Switch(config)#no autosave enable
Switch(config)#copy config nvram
```

2. Enable MAC security and auto-learning on ports 1/6-14.

```
Switch(config)#interface Ethernet 1/6-14
Switch(config-if)#mac-security enable
Switch(config-if)#mac-security auto-learning enable
Switch(config-if)#mac-security auto-learning max-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

Port  Trunk  Security  Auto-Learning  MAC Number
----  -----  --------  -------------  ----------
   6         Disabled     Disabled        2
   7         Disabled     Disabled        2
   8         Disabled     Disabled        2
   9         Disabled     Disabled        2
  10         Disabled     Disabled        2
  11         Disabled     Disabled        2
  12         Disabled     Disabled        2
  13         Disabled     Disabled        2
  14         Disabled     Disabled        2
```

4. Connect a PC to port 1/8 and verify the configuration by displaying the MAC security MAC address table.

```
Switch#show mac-security mac-address-table
Number of addresses: 1
Port Allowed MAC Address   Type
---- ------------------- ---------
8        00-02-A5-E9-00-28     Sticky

Security List Allowed MAC Address   Type
------------- ------------------- ---------

Trunk Allowed      MAC Address       Type
 -------------- ------------------- ---------
```

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.

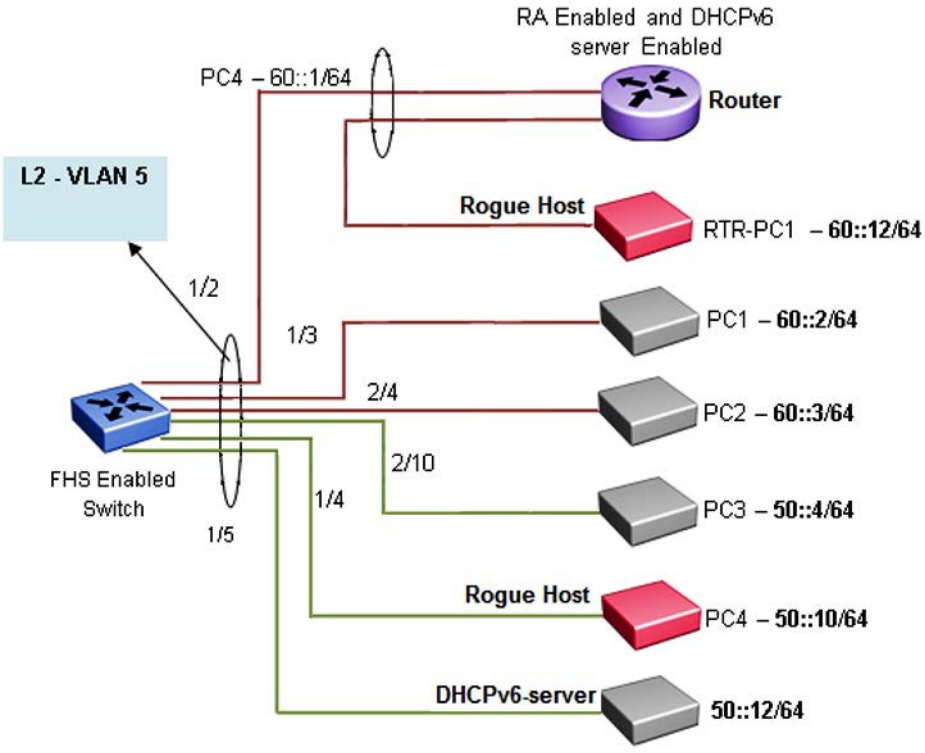

Figure 19: FHS deployment topology

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.

Create 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.

Create 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
   ```

Create 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
   ```

Create 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
   ```

Create 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
   ```

Create 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
   ```

Create 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
   ```

Attach 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
```

Enable 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
```