

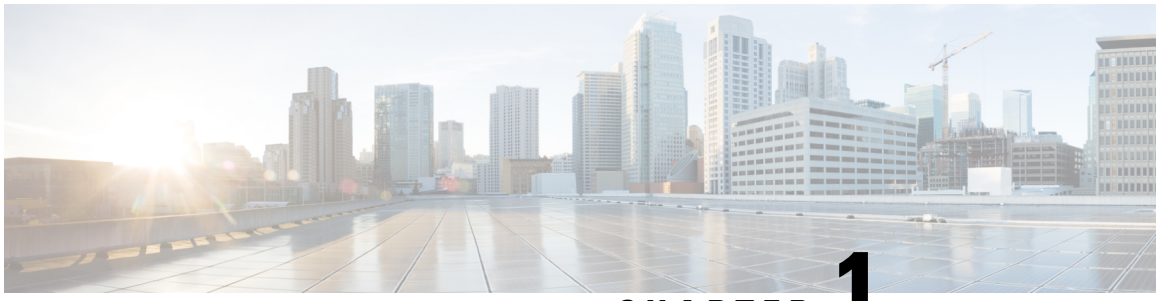
Cisco Business 350 Series Switches Administration Guide

First Published: 2020-05-07

Last Modified: 2024-06-27

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2024 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Get To Know Your Switch

This chapter contains the following sections:

- Introduction, on page 1
- Rack Mounting Switch, on page 2
- Wall Mounting a Switch, on page 3
- Out-Of-Band Port, on page 6
- Stacking the Switches, on page 6
- Power over Ethernet Considerations, on page 8
- Front Panel, on page 10
- Configuring Switches, on page 13
- Navigation, on page 16

Introduction

Thank you for purchasing the Cisco CBS Series Switch. The Cisco CBS Series Switches combine powerful network performance and reliability with a complete suite of network features that you need for a solid business network. These expandable Gigabit Ethernet switches, with Gigabit or 10-Gigabit uplinks, provide multiple management options, rich security capabilities, and Layer-3 static routing features far beyond those of an unmanaged or consumer-grade switch, at a lower cost than fully managed switches.

Before You Begin

Before you begin installing your device, ensure that the following items are available:

- RJ-45 Ethernet cables for connecting network devices. A category 6a and higher cable is required for 10G ports; a category 5e and higher cable is required for all other ports.
- Tools for installing the hardware.
  - The rack-mount kit packed with the switch contains four rubber feet for desktop placement, and two brackets and twelve screws for rack mounting.
  - If the supplied screws are lost, use replacement screws in the following size:
    - Diameter of the screw head: 6.9 mm
    - Length of the face of the screw head to the base of screw: 5.9 mm
    - Shaft diameter: 3.94 mm

Warning To prevent airflow restriction, allow clearance around the ventilation openings to be at least 3 inches (7.6 cm).

- A computer to manage the device either via the console port or via the web-based interface. for web-based interface the computer needs to support one of the following browsers:
  - Microsoft Edge
  - Firefox (version 82 or 81 or higher)
  - Chrome (version 86 or 85 or higher)
  - Safari over MAC (version 14.0 and higher)

Warning Suitable for installation in information Technology Rooms in accordance with Article 645 of the national Electric Code and NFPA 75.

Rack Mounting Switch

You can mount the switches on any standard size, 19-inch (about 48 cm) wide rack. The switch requires 1 rack unit (RU) of space, which is 1.75 inches (44.45 mm) high.

Caution For stability, load the rack from the bottom to the top, with the heaviest devices on the bottom. A top-heavy rack is likely to be unstable and might tip over.

To install the switch into a 19-inch standard chassis:

Procedure

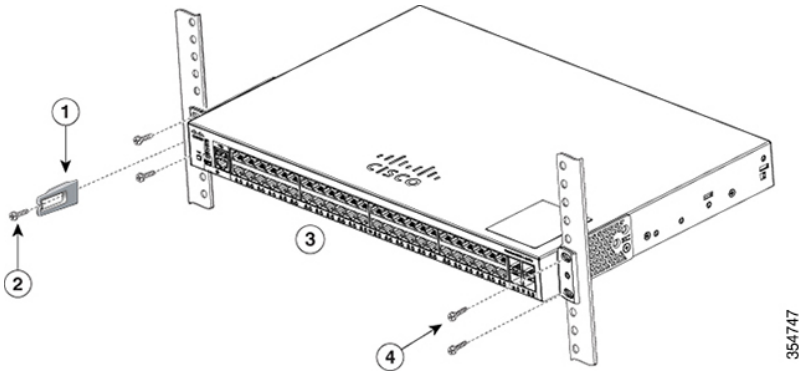
Step 1 Place one of the supplied brackets on the side of the switch so that the four holes of the brackets align to the screw holes, and then use the four supplied screws to secure it.

Step 2 Repeat the previous step to attach the other bracket to the opposite side of the switch.

Step 3 After the brackets are securely attached, the switch is now ready to be installed into a standard 19-inch rack.

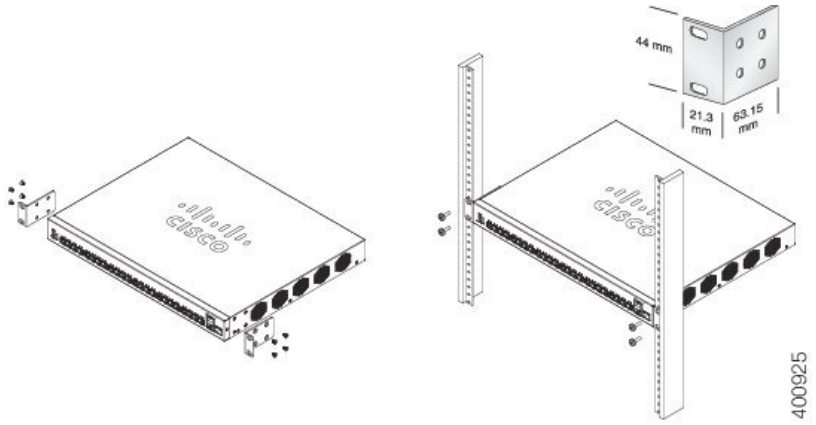
Note Use supplied brackets to rack mount the switch.

Supplied rack mounting for switch models with front mounting position. The mounting ears do not sit flush to the front panel.



Due to design differences, some of the mounting brackets will attach such that the switch will protrude about an inch from the mounting surface.

Supplied rack mounting for switch models with front mounting position. The mounting ears sit flush to the front panel.



Wall Mounting a Switch

You can mount the switches on a wall, using wall studs or to a firmly attached plywood mounting backboard.

Caution Read these instructions carefully before beginning installation. Failure to use the correct hardware or to follow the correct procedures could result in a hazardous situation to people and damage to the system.

Caution Do not wall-mount the switch with its front panel facing up. Following safety regulations, wall mount the switch with its front panel facing down or to the side to prevent airflow restriction and to provide easier access to the cables.

To wall-mount a 24-port switch using brackets:

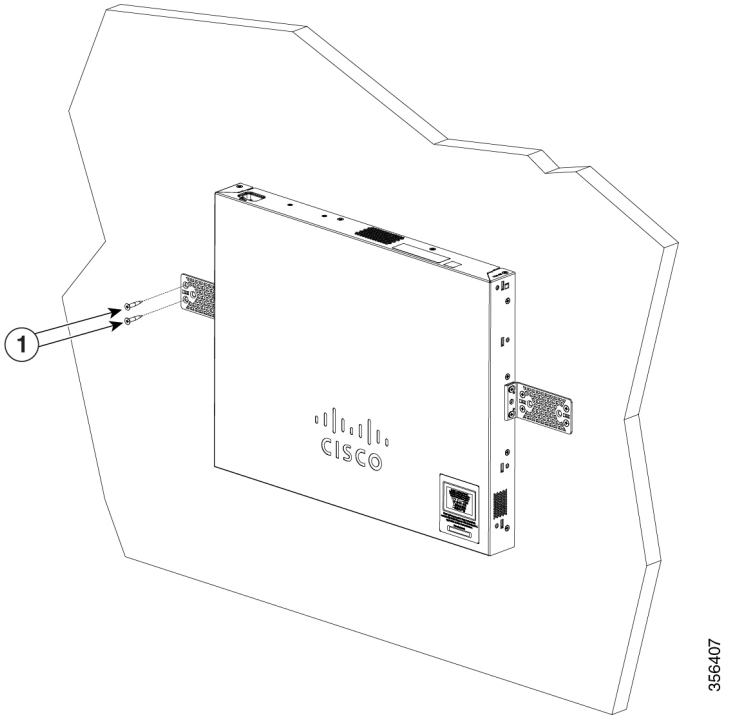
Procedure

Step 1 Attach a 19-inch bracket to one side of the switch.

Step 2 Repeat the previous step to attach the other bracket to the opposite side of the switch.

Step 3 After the brackets are securely attached, mount the switch with the front panel facing down. Make sure that the switch is attached securely to wall studs or to a firmly attached plywood-mounting backboard. Wall-mounting a 24-port switch.

Wall-mounting a 24-port



Wall Mount an 8 Port Switch

To wall-mount a 8-port switch using mounting screws, follow these steps:

Procedure

Step 1 Locate the screw template. The template is used to align the mounting screw holes.

Step 2 Position the screw template so that the edge that is marked as CABLE SIDE ENTRY faces toward the floor. Make sure that the switch is attached securely to wall studs or to a firmly attached plywood mounting backboard.

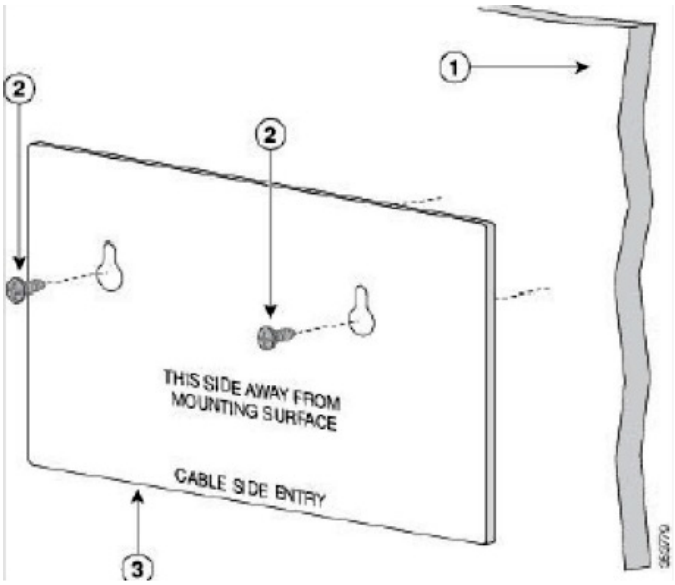
Step 3 Peel the adhesive strip off the bottom of the screw template.

Step 4 Attach the screw template to the wall.

Step 5 Use a 0.144-inch (3.7 mm) or a #27 drill bit to drill a 1/2-inch (12.7 mm) hole in the two screw template slots.

Step 6 Insert two screws in the slots on the screw template and tighten them until they touch the top of the screw template. Installing the mounting screws on the wall

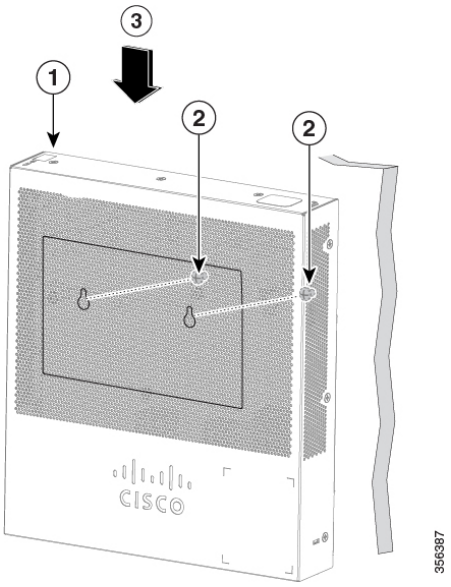
Figure 3 Installing the mounting screws on the wall



Step 7 Remove the screw template from the wall.

Step 8 Place the switch onto the mounting screws, and slide it down until it locks in place. Wall-mounting an 8-port switch

Figure 4 Wall-mounting an 8-port switch



Out-Of-Band Port

The CBS350 “10G network port SKUs” support an Out-of-Band (OOB) port which can be used for the management network. The out-of-band and the in-band ports share the same IP routing table. Thus, the same subnet cannot be used on both the in-band and out-of-band interfaces.

The OOB port is assigned a MAC address which differs from the base MAC address and the in-band ports addresses. This MAC address is used as the source MAC address in all frames sent by the switch on the OOB port.

By default, VLAN 1 is configured with a default IP address 192.168.1.254, and can be accessed through any in-band interfaces. This default IP address is used when no other address is assigned (dynamically or statically). There is no default IP address on OOB port.

Table 1: VLAN 1 and OOB Factory Default IP settings – Old and new behavior

	Cisco Business firmware up to version 3.1		**Cisco Business firmware version 3.1.1**	
	OOB interface	VLAN 1 interface	OOB interface	VLAN 1 interface
IP settings	Default IP + DHCP		DHCP enable	Default IP + DHCP
Interface CLI configuration	None	None	"IP address DHCP"	None
Other	Bonjour enabled	None	None	Bonjour enabled

Stacking the Switches

A stack can have multiple devices in it. Any 10G port of the switch can be used for stacking.

By default, the ports on the switch function as regular Ethernet ports, except if you configure them to do stacking. You cannot mix the stack speeds between the switches or ports.

At least two ports must be chosen for stacking in a given switch" and those ports must be 10Gig speed. For two switches or more to form a stack, they must be running the same version of the firmware. This is the more reason SG series switches cannot be stacked with CBS series switches. CBS250 series switches do not have stacking capabilities.

Some switches have their stack LEDs numbered 1, 2, 3, and 4 to indicate Active, Standby, and Member while the others types use the system LED flashing behavior to describe the same thing.



Note Stack ports must have the same speed capability on the module or cable plug in.

The switch can only be stacked without Mesh topology. The switches in the same stack are connected together through their stack ports. Depending on the type of stack ports and the desired speed, you may need Cat6a Ethernet cables or Cisco approved modules or cables for the switches.

Some network switches have the ability to be connected to other switches and operate together as a single unit. These configurations are called stacks, and they are useful for quickly increasing the capacity of your network.

Stack Management

The Cisco Business switches have a couple of different stacking modes, and you can stack different models.

Also, you need to note what feature may or may not be available in different stacking modes (native or hybrid).

- Native Stacking- The switch is part of a stack in which all of the units are of the same type.
- Hybrid Stacking – The switch is part of a stack that can consist of either mixed type of CBS350 devices.

Cisco Business Switch Stacking Mode Selector

This tool will guide you to selecting the correct stacking settings for your 10G Cisco Business 350 series switch. Click on the link below to access the tool.

https://www.cisco.com/c/en/us/support/docs/smb/switches/Cisco-Business-Switching/kmgmt-2799-switch-stack-selector-cbs.html

Note You cannot stack the legacy switches with the new Cisco Business stackable switches. If you are stacking the legacy switches, consult the following link: https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-350x-series-stackable-managed-switches/smb5367-feature-support-comparison-between-the-cisco-stackable-manag.html

Feature Support on Hybrid Mode

The feature set of the CBS350 SKUs with 10G network ports and the feature CBS350 SKUs with 10G uplink ports are nearly identical. However, there are a few differences in feature support and table sizes between the 2 “sub-types”. The Cisco Business switches hybrid stack mode will support the lower denominator for these features/tables The following table lists the feature differences between the 2 sub-types and the setting applied in hybrid mode:

Hybrid mode works in any combination of stacking albeit reduced performance, MAC table size for example can be reduced; but switches of the same model number (same PID) can take advantage of native stacking mode. Some switches with different PID can stack in native mode as well, other combinations, however, can only stack in hybrid mode.

In general, except for the CBS350-48XT-4X, all CBS350 switches that support stacking and have designated uplink ports in their PID can stack natively among themselves, and those that do not have uplink ports, including the CBS350-48T-4X can stack, among themselves, in native mode as well. The hybrid mode staking comes into play only when mixing these two blocks, uplink supporting devices and non-uplink supporting devices. So. knowing the exact PID of a given switch is so crucial when it comes to stacking mode determination. The CBS350-48T-4X, although has 4X at the end of the PID that should designate this as supporting an uplink, it is not the case, this 4X designation in this switch does not indicate uplink, instead, they are network port (downlink port) as are the other ports in the switch.

Changing stacking mode from Native to Hybrid will force a switch to reboot and most of its settings in its startup configuration will reset to default; on the other hand, changing the stacking mode from Hybrid to Native will force the unit to reboot, but the settings will not reset back to default.

Feature	CBS350 "10G uplink port SKUs"	CBS350 "10G network port SKUs"	Hybrid stack
OOB port	Not Supported	Supported	Not Supported
Green Settings (Short reach and Energy Detect)	Per SKU and port type behavior	Per SKU and port type behavior	Per SKU and port type behavior
MAC table size	16K	32K or 64K	16K
Number of Multicast groups	2K	4K	2K
Number of ACEs supported	1K- reserved	2K- reserved	1K- reserved
Total number of IP entries	992	7392	992
ARP table size	1K – reserved	8K – reserved	1K – reserved
Max number of IPv6 interfaces	106	200	106
Max MAC table aging	400 seconds	630 seconds	400 seconds
IPv6 Manual Tunnel/ 6tp4 tunnel/ ISATAP routing tunnel	Not supported	Supported	Not supported
PoE support	Supported on specific SKUs	Not supported	Per SKU type
Default number of VLAN Mapping entries	0	32	0
Default IP address	On VLAN 1	On VLAN 1	On VLAN 1

Power over Ethernet Considerations

Some switches support PoE while others do not. The switch models that support PoE have a P in their model number, such as: CBSxxx-xxP-xx. If your switch is one of the Power over Ethernet (PoE) models, consider the following power requirement.

Warning The switch is to be connected only to PoE networks without routing to the outside plant.

Table 2: Switches with Power Over Ethernet

SKU Name	Description	PoE PD Chipset Type	PoE PSE Support
CBS350-8MGP-2X	8-Port 2.5G PoE Managed Switch	1*69208M	AF/AT

SKU Name	Description	PoE PD Chipset Type	PoE PSE Support
CBS350-8MP-2X	8-Port 2.5G PoE Stackable Managed Switch	1*69208M	AF/AT
CBS350-24MGP-4X	24-Port 2.5G PoE Stackable Managed Switch	1*69208M + 1*69204	AF/AT/60W
CBS350-12NP-4X	12-Port 5G PoE Stackable Managed Switch	3 * TPS2388	AF/AT/60W
CBS350-24NGP-4X	24-Port 5G PoE Stackable Managed Switch	4* TPS2388	AF/AT/60W
CBS350-48NGP-4X	48-Port 5G PoE Stackable Managed Switch	7* TPS2388	AF/AT /60W
CBS350-8P-2G	8-Port Gigabit PoE Managed Switch	TPS2388	AF/AT
CBS350-8P-E-2G	8-Port Gigabit PoE Managed Switch	TPS2388	AF/AT
CBS350-8FP-2G	8-Port Gigabit PoE Managed Switch	TPS2388	AF/AT
CBS350-8FP-E-2G	8-Port Gigabit PoE Managed Switch	TPS2388	AF/AT
CBS350-16P-2G	16-Port Gigabit PoE Managed Switch	2*TPS2388	AF/AT
CBS350-16P-E-2G	16-Port Gigabit PoE Managed Switch	2*TPS2388	AF/AT
CBS350-16FP-2G	16-Port Gigabit PoE Managed Switch	2*TPS2388	AF/AT
CBS350-24P-4G	24-Port Gigabit PoE Managed Switch	3*TPS2388	AF/AT
CBS350-24FP-4G	24-Port Gigabit PoE Managed Switch	3*TPS2388	AF/AT
CBS350-48P-4G	24-Port Gigabit PoE Managed Switch	6*TPS2388	AF/AT
CBS350-48FP-4G	48-Port Gigabit PoE Managed Switch	6*TPS2388	AF/AT
CBS350-24P-4X	24-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks	3*TPS2388	AF/AT
CBS350-24P-4X	24-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks	3*TPS2388	AF/AT
CBS350-24FP-4X	48-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks	6*TPS2388	AF/AT
CBS350-48P-4X	48-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks	6*TPS2388	AF/AT
CBS350-48FP-4X	48-Port Gigabit PoE Stackable Managed Switch with 10G Uplinks	6*TPS2388	AF/AT

Caution Consider the following when connecting a PoE switch. The PoE switches are PSE (Power Sourcing Equipment) that are capable of supplying DC power to attaching powered devices (PD). These devices include VoIP phones, IP cameras, and wireless access points. The PoE switches can detect and supply power to pre-standard legacy PoE PD. Due to the PoE legacy support, it is possible that a PoE switch acting as a PSE may mistakenly detect and supply power to an attaching PSE, including other PoE switches, as a legacy PD. Even though PoE switches are PSE, and as such should be powered by AC, they could be powered up as a legacy PD by another PSE due to false detection. When this happens, the PoE switch may not operate properly and may not be able to properly supply power to its attaching PDs.

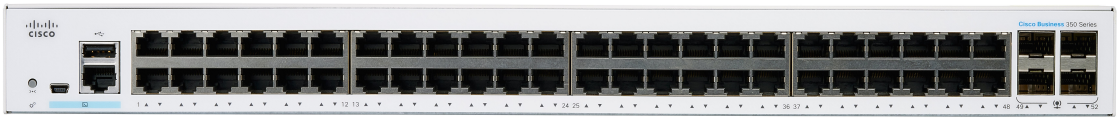
To prevent false detection, you should disable PoE on the ports on the PoE switches that are used to connect to PSEs. You should also first power up a PSE device before connecting it to a PoE switch. When a device is being falsely detected as a PD, you should disconnect the device from the PoE port and power recycle the device with AC power before reconnecting its PoE ports.

Front Panel

The ports, LEDs, and Reset button are located on the front panel of the switch, as well as the following components:



Cisco Business 350 Series Model



Note Models may differ within the CBS 350 series and this is just a representation of a model within the series.

- There are 2 device types with different console interface:
  - Console port with RJ-45 and mini USB connector if both are connected the Mini USB has precedence over the RJ-45
  - RJ-45 connector only type of console.

The console interface connects a serial cable to a computer serial port so that it can be configured using a terminal emulation program or mini USB cable (depending on the connector).

- USB Port—The USB port connects the switch to a USB device so that you can save and restore the configuration files, firmware images, and SYSLOG files through the connected USB device. The USB port supports the FAT32 file system.
- RJ-45 Ethernet Ports—The RJ-45 Ethernet ports connect network devices, such as computers, printers, and access points, to the switch.
- SFP+ Port (if present)—The small form-factor pluggable plus (SFP+) are connection points for modules so that the switch can link to other switches. These ports are also commonly referred to as mini 10GigaBit Interface Converter ports. The term SFP+ is used in this guide.
  - The SFP+ ports (if present) are compatible with the following Cisco SFP 1G optical modules MGBSX1, MGBLX1, MGBLH1, MGBT1, as well as other brands.
  - The SFP+ ports are compatible with the following Cisco SFP 1G optical modules MGBSX1, MGBLX1, MGBLH1, MGBT1, as well as other brands.
  - The Cisco SFP+ Copper Cable modules that are supported in the Cisco switches are: SFP-H10GB-CU1M, SFP-H10GB-CU3M, and SFP-H10GB-CU5M.
  - The LEDs of the corresponding RJ-45 port flash green to respond to the SFP interface traffic.
- Small form-factor pluggable (SFP) ports are connection points for modules, so the switch can link to other switches.
- Some SFP interfaces are shared with one other RJ-45 and SFP+ port, called a combo port. When the SFP is active, the adjacent RJ-45 port is disabled.
- Reset button is used to reset or reboot the switch. The table below displays the reset behavior on the switch.

Press Type	New Behavior (Firmware 3.2 and on)	Old Behavior (Firmware prior to 3.2)
1- 5 seconds	System LED is green, releasing button does not cause reload.	Reload
6- 10 seconds	System LED flash green, releasing button during this period will cause device reload, but system is not set to factory default.	Reload
11-15 seconds	System LED is green, releasing button does not cause reload	Factory default
16-20 seconds	System LED flashes green, releasing button during this period will cause device reload to factory default	Factory default
> 20 seconds	System LED is green, releasing button does not cause reload	Factory default

Note Stack Behavior

The reset button disable setting is applied to all units in the stack, meaning that if configured, the reset button on all units in the stack are disabled, and if not configured the reset button on all units in the stack are enabled. This applies also to units that join an existing stack.

- OOB Port (if present)—The Out of Band (OOB) port is a CPU Ethernet port that can be used only as a management interface. Bridging between the OOB port and the in-band Layer 2 interface is not supported. This does not appear on 250 devices.
- Multi-Gigabit Ethernet Ports (if present) —Highlighted in blue, these ports support speeds up to 2.5 Gbps or 5 Gbps on Cat5e cables. The maximum speed supported is printed on the blue shade under the port. Uplink ports on CBS350-8MGP-2X also support multi-Gigabit speed. In this case, port speed can reach 10Gbps. Most of the cabling deployed worldwide is Cat5e, and previously limited to 1 Gbps at 100 meters. Cisco multi-Gigabit Ethernet enables speeds up to 2.5 or 5 Gbps on the same infrastructure without replacing a cable.
- 60-Watt PoE Ports (if present)- The 60-Watt PoE port doubles the maximum PoE power delivered on the port to 60W.

Front Panel LEDs

The following are the global LEDs found on the devices:

- System—(Green) The LED lights steady when the switch is powered on, and flashes when booting, performing self-tests, or acquiring an IP address. If the LED flashes Amber, the switch has detected a hardware or firmware failure, and/or a configuration file error.

The following LEDs describe the stacking status of the unit.

- *Stack ID LED (Green)- The LED lights steady when the switch is stacked and the corresponding number indicates its Stack ID.
- *Active Unit ID LED- indicating this is the stack active unit.

Note * These two LEDs are only available on certain models.

- System LED- Every 20 seconds, the System LED will flash according to unit ID of the member unit.
  - Flash = LED going off and then on again.
  - According to unit ID of the unit. This means
    - Unit 1 (if not active unit)- system LED will flash 1 time
    - Unit 2 (if not active unit)- system LED will flash 2 times
    - Unit 3- system LED will flash 3 times
    - Unit 4-system LED will flash 4 times;

- The duration of each flash (LED off time) will be as follows:
  - LED off time (in each flash) ~ 0.5 seconds.
  - “Interim” LED on (between 2 LED offs) ~ 0.5 seconds
- If a member unit is removed from the stack, its system LED will continue to flash according to above definition.

The following are per port LEDs:

- LINK/ACT—(Green) Located on the left of each port. The LED lights steady when a link between the corresponding port and another device is detected, and flashes when the port is passing traffic.
- SFP+ (if present)—(Green) Located on the right of a 10G port. The LED lights steady when a connection is made through the shared port, and flashes when the port is passing traffic.
- XG—(Green) Located on the right of a 10G port. The LED lights steady when another device is connected to the port, is powered on, and a 10 Gbps link is established between the devices. When the LED is off, the connection speed is under 10 Gbps or nothing is cabled to the port.
- Gigabit—(Green) Located on the right of the 1G port. The LED lights steady when another device is connected to the port, is powered on, and a 1000 Mbps link is established between the devices. When the LED is off, the connection speed is under 1000 Mbps or nothing is cabled to the port. (This feature is only available on certain models).
- PoE (if present)—(Amber) Located on the right of the port. The LED lights steady when power is being supplied to a device attached to the corresponding port. (This feature is only available on certain models).

Configuring Switches

The switch can be accessed and managed over your IP network using the web-based interface, or by using the switch’s command-line interface through the console port. Using the console port requires advanced user skills and is only supported on certain models.

The following table shows the default settings used when configuring your switch for the first time.

Parameter	Default Value
Username	cisco
Password	cisco
LAN IP	192.168.1.254

Configuring Your Switch Using the Web-based Interface

To access the switch with a web-based interface, you must know the IP address that the switch is using. The switch uses the factory default IP address of 192.168.1.254, with a subnet of /24. When the switch is using the factory default IP address, the System LED flashes continuously. When the switch is using a DHCP server-assigned IP address or an administrator has configured a static IP address, the System LED is a steady green (DHCP is enabled by default).

If you are managing the switch through a network connection and the switch IP address is changed, either by a DHCP server or manually, your access to the switch will be lost. You must enter the new IP address that the switch is using into your browser to use the web-based interface. If you are managing the switch through a console port connection, the link is retained.

To configure the switch using the web-based interface:

Procedure

Step 1 Power on the computer and your switch.

Step 2 Connect the computer to any network port.

Step 3 Set up the IP configuration on your computer.

a) If the switch is using the default static IP address of 192.168.1.254/24, you must choose an IP address for the computer in the range of 192.168.1.2 to 192.168.1.253 that is not already in use.

b) If the IP addresses will be assigned by DHCP, make sure that your DHCP server is running and can be reached from the switch and the computer. You may need to disconnect and reconnect the devices for them to discover their new IP addresses from the DHCP server.

Note
Details on how to change the IP address on your computer depend upon the type of architecture and operating system that you are using. Use your computers local Help and Support functionality and search for "IP Addressing."

Step 4 Open a web browser window.

Step 5 Enter the switch IP address in the address bar and press **Enter**. For example, http://192.168.1.254.

Step 6 When the login page appears, choose the language that you prefer to use in the web-based interface and enter the username and password.

The default username is cisco. The default password is cisco. Usernames and passwords are both case sensitive.

Step 7 Click **Log In**.

Step 8 If this is the first time that you have logged on with the default username and password, the Change username and Password. Enter a new username and password and confirm.

If this is the first time that you have logged on with the default username and password, the Change username and Password

page opens

Note
Please refer to the password complexity rule section in Login Settings, on page 262 before creating a password.

Step 9 Click **Apply**.

Caution
Make sure that any configuration changes made are saved before exiting from the web-based interface by clicking on the Save icon. Exiting before you save your configuration results in all changes being lost.

The Getting Started page opens. You are now ready to configure the switch. Refer to the Administration Guide or see the help pages for further information.

Configuring Your Switch Using the Console Port

To configure the switch using the console port, which is only supported on certain models, proceed with the following steps:

Procedure

Step 1 Connect a computer to the switch console port using a Cisco console cable (purchased separately) or a cable with mini USB connector.

Step 2 Start a console port utility such as Hyper Terminal on the computer.

Step 3 Configure the utility with the following parameters:

- 115200 bits per second
- 8 data bits
- no parity
- 1 stop bit
- no flow control

Step 4 Enter a username and password. The default username is cisco, and the default password is cisco. Usernames and passwords are both case sensitive.

If this is the first time that you have logged on with the default username and password, the following message appears:

```
Please change your username AND password from the default settings. Change of credentials
 is required for better protection of your network.
Please note that new password must follow password complexity rules
```

Step 5 Set a new administrator username and password.

Caution
Make sure that any configuration changes made are saved before exiting.

You are now ready to configure the switch. See the CLI Guide for your switch.

Note
If you are not using DHCP on your network, set the IP address type on the switch to Static and change the static IP address and subnet mask to match your network topology. Failure to do so may result in multiple switches using the same factory default IP address of 192.168.1.254.

Console access also provides additional interfaces for debug access which are not available via the web interface. These debug access interfaces are intended to be used by a Cisco Support Team personnel, in cases where it is required to debug device's behavior. These interfaces are password protected. The passwords are held by the Cisco support team. The device supports the following debug access interfaces:

- U-BOOT access during boot sequence
- Linux Kernel access during boot sequence

- Run time debug modes- allows Cisco support team to view device settings and apply protocol and layer 1 debug commands and settings. The run time debug mode is accessible over telnet and SSH terminals in addition to the console.

Navigation

The navigation menu, located at the top right of each UI page, lists the device's main features. You can access each feature's UI pages using a series of cascading menus. To access an individual UI page, click the corresponding feature tab in the navigation menu to display a menu of subcategories. Select a subcategory and repeat this process until you see the desired page, and then select the page to display it in the main window.

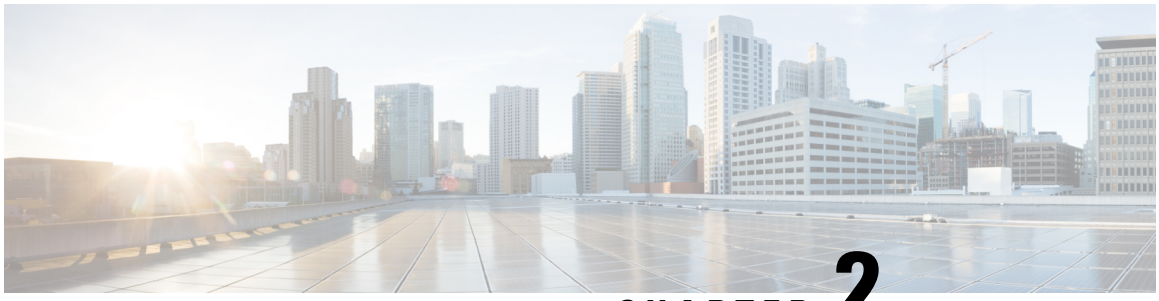
Basic or Advanced Display Mode

The product supports many features, and therefore the WEB GUI includes hundreds of configuration and display pages. These pages are divided into the following display modes:

- Basic—Basic subset of configuration options are available. If you are missing some configuration option, select the Advanced mode in the device header.
- Advanced—Full set of configuration options are available.

When the user switches from basic to advanced, the browser reloads the page. However, after reloading, the user stays on the same page. When the user switches from advanced to basic, the browser reloads the page. If the page exists also on the basic mode, the user stays on the same page. If the page does not exist in the basic mode, the browser will load the first page of the folder which was used by the user. If the folder does not exist, the Getting Started page will be displayed.

If there is an advanced configuration, and the page is loaded in basic mode, a page-level message will be displayed to the user (e.g, there are 2 radius servers configured but in basic mode only a single server can be displayed, or there is 802.1X port authentication with time range configured but time range is not visible in basic mode). When switching from one mode to another, any configuration which was made on the page (without Apply) is deleted.



CHAPTER 2

Getting Started

This chapter contains the following section:

- Getting Started, on page 17

Getting Started

This section will guide you on how to install and manage your device.

Click on **Getting Started** to access the page where you can use the various links and follow the on-screen instructions to quickly configure your switch.

Basic or Advanced Display Mode

The switch's WEB GUI includes hundreds of configuration and display pages. These pages are divided into the following display modes:

- Basic—Basic subset of configuration options.
- Advanced—Full set of configuration options are available

When switching from one mode to another, any configuration which was made on the page (without Apply) is deleted.

Initial Setup

Manage Stack	Stack Management, on page 61
Change Management Applications and Services	TCP/UDP Services, on page 284
Change Device IP Address	IPv4 Interface, on page 201
Create VLAN	VLAN Settings, on page 143
Configure Port Settings	Port Settings, on page 119

Device Status

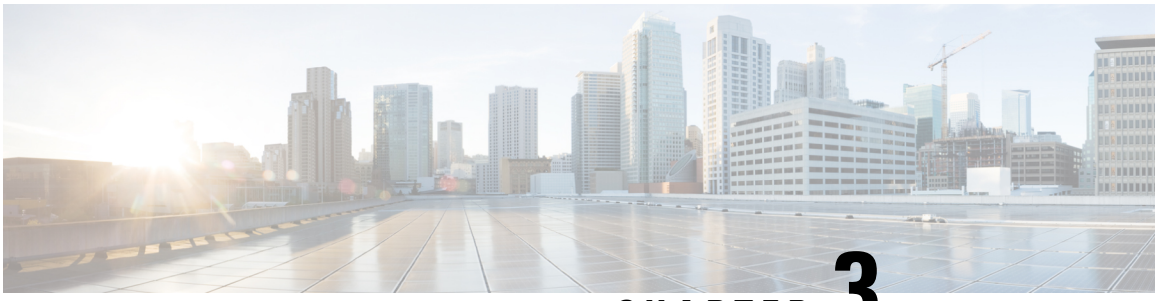
System Summary	System Summary, on page 33

Port Statistics	Interface, on page 36
RMON Statistics	Statistics, on page 50
View Log	RAM Memory, on page 57

Quick Access

Change Device Password	User Accounts, on page 62
Upgrade Device Software	Firmware Operations, on page 74
Backup Device Configuration	File Operations, on page 76
Create MAC-Based ACL	MAC-Based ACL, on page 329
Create IP-Based ACL	IPv4-based ACL, on page 331
Configure QoS	QoS Properties, on page 341
Configure SPAN	SPAN and RSPAN , on page 44

There are four hot links on the Getting Started page that take you to Cisco web pages for more information. Clicking on the Support link takes you to the device product support page, and clicking on the Forums link takes you to the Support Community page. Clicking on the **Virtual Assistant** will take you to the virtual assistant where you can ask your questions and clicking on CBD will take you to the Cisco Business Dashboard application where you can manage your network.



CHAPTER 3

Dashboard

This chapter contains the following section:

- Dashboard, on page 19

Dashboard

The dashboard is a collection of 8 squares, initially empty, that can be populated by various types of information. You can select a number of modules from the available modules and place them in this grid. You can also customize settings of the currently displayed modules. When the dashboard loads, the modules you selected for the dashboard are loaded in their locations in the grid. The data in the modules is updated, in intervals depending on the module type.

When you open the dashboard, a wire frame view of the grid is displayed. To display modules that aren't currently being displayed, click **Customize**. Add modules by selecting a module from the list of modules on the right and dragging and dropping it to any space in the grid.

The modules are divided into the following groups:

- Small Modules are modules that take up a single square.
- Large Modules take up two squares.

If you drag a module into a space currently occupied, the new module replaces the previous one. You can rearrange the placement of the modules in the grid by dragging a module from one occupied grid position to another position. Only when you click **Done** are the modules populated by the relevant information. The title bar of each module in the dashboard displays the title of the module and three buttons.

- Pencil — Opens configuration options (depending on the module).
- Refresh — Refreshes the information.
- X — Removes the module from the dashboard.

Table 3: Small Modules

System Health	The System Health displays information about device health.
	• Fan Status
	  • Yellow— A fan has failed and is backed up by a redundant fan.
	  • Green—Fan is operational.
	  • Red—Fan is faulty.
	• Thermometer Status
	  • Green —Temperature is OK.
	  • Yellow—Temperature generates a warning.
	  • Red—Temperature is critical.

Resource Utilization	This module displays the utilization status in terms of a percentage of the various system resources as a bar chart The resources monitored are: • Multicast Groups—Percentage of Multicast groups that exist out of the maximum possible number that are permitted to be defined. • MAC Address Table—Percentage of MAC Address table in use. • TCAM—Percentage of TCAM used by QoS and ACL entries. • CPU—Percentage of CPU being used.
Identification	This module displays basic information regarding the device. It displays the following fields: • System Description—Displays description of the device. • Host Name—Entered in the System Settings, on page 59 or default is used. • Firmware Version—Current firmware version running on device. • MAC Address—MAC address of the device. • Serial Number—Serial number of the device. • System Location (if configured)—Enter the physical location of the device. • System Contact (if configured)—Enter the name of a contact person. • Total Available Power (for PoE devices only)—Amount of power available to the device. • Current Power Consumption (for PoE devices only)—Amount of power consumed by the device.

PoE Utilization	This module displays a graphic representation of the PoE utilization status. For a standalone unit, this module displays a gauge with a dial of values from 0-100. The section of the dial from the traps threshold to 100 is red. In the middle of the gauge, the actual PoE utilization value is shown in watts. Each bar represents the PoE utilization percentage value of the device on a scale of 0 to 100. If the PoE utilization is higher than the traps threshold, the bar is red. Otherwise the bar is green. When hovering on a bar, a tool tip appears showing the actual PoE utilization of the device in watts. Additional views can be selected in the configuration options (pencil icon in upper-right corner). • Refresh Time—Select one of the displayed options. • PoE Global Properties—Link to the **Port Management > PoE > Properties** page. • PoE Port Settings—Link to the **Port Management > PoE > Settings** page. **Note** This section is only relevant for devices supporting PoE.

Table 4: Large Modules

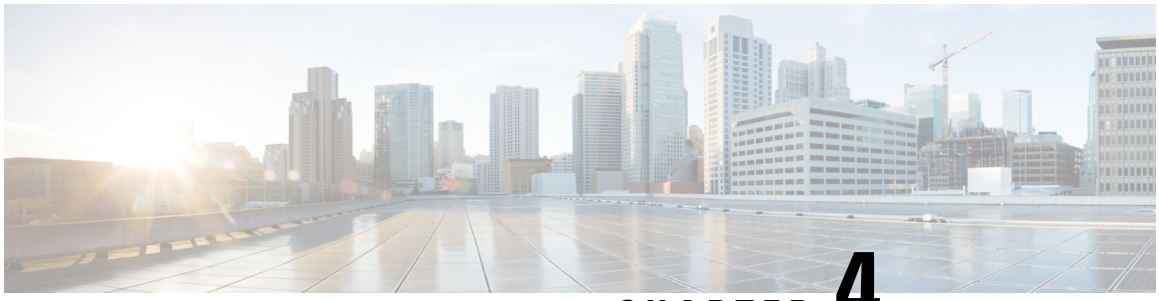
Latest Logs	This module contains information about the five latest events logged by the system as SYSLOGs. The following configuration options (right-hand corner) are available: • Severity Threshold—Described in Log Settings, on page 71. • Refresh Time—Select one of the options displayed. • View logs—Click to open RAM Memory, on page 57 .

Suspended Interfaces	This module displays interfaces that have been suspended in either device or table view. The view is selected in the configuration options-Display Option (pencil icon in upper-right corner).
	• Device View—In this view, the device is displayed. When units are connected in a stack, a drop-down selector enables the user to select the device to be viewed. All suspended ports in the device are shown as red.
	• Table View—In this view, there is no need to select a specific stack unit. Information is displayed in table form as follows:
	  • Interface—Port or LAG that was suspended
	  • Suspension Reason—Reason interface was suspended
	  • Auto-recovery current status—Has auto recovery been enable for the feature that caused the suspension.
	The following configuration options (right-hand corner) are available:
	• Refresh Time—Select one of the options displayed
	• Error Recovery Settings—Click to open Error Recovery Settings, on page 122.

Stack Topology	This module is a graphic representation of the stack topology and is identical in behavior to the Stack Topology View. It displays the following fields: • Stack Topology—Either Chain or Ring. • Stack Active Unit—Number of unit functioning as the active unit of the stack. Hovering over a unit in the module displays a tool tip identifying the unit and providing basic information on its stacking ports. Hovering over a stack connection in the module displays a tool tip detailing the connected units and the stacking ports generating the connection.

Port Utilization	This section displays the port utilization on the device. The view is selected in the configuration options (pencil icon in upper-right corner).
	• Display Mode—Device View- Displays the device Hovering over a port displays information about it.
	• Display Mode—Chart View- A list of ports and how they are being used is displayed. For each port, the following port utilization information can be viewed.
	  • Tx—% (red)
	  • Rx—% (blue)
	• Refresh Time—Select one of the displayed options.
	• Interface Statistics—Link to the **Status and Statistics > Interface**.

Traffic Errors	This module displays the number of error packets of various types that are counted on the RMON statistics. The view is selected in the configuration options (pencil icon in upper-right corner).
	• Display Mode- Device View
	  The device module mode displays a diagram of the device. All suspended ports in the device are shown as red.
	  Hovering over a suspended port displays a tool tip with the following information:
	  • Port name.
	  • If the port is a member of a LAG, the LAG identity of the port.
	  • Details of the last error logged on the port.
	• Display Mode- Table View
	  • Interface—Name of port
	  • Last Traffic Error—Traffic error that occurred on a port and the last time the error occurred.
	• Refresh Time—Select one of the refresh rates.
	• Traffic Error Information—Click to link to the Statistics, on page 50.



CHAPTER 4

Configuration Wizards

This chapter contains the following sections:

- Getting Started Wizard, on page 25
- VLAN Configuration Wizard, on page 26
- ACL Configuration Wizard, on page 27

Getting Started Wizard

The Getting Started Wizard will assist you in the initial configuration of the device.

Procedure

Step 1 In **Configuration Wizards** > **Getting Started Wizard**, click **Launch Wizard.**

Step 2 Click **Launch Wizard** and Next.

Step 3 Enter the fields in the General Information tab:

- System Location—Enter the physical location of the device.
- System Contact—Enter the name of a contact person.
- Host Name—Select the host name of this device. This is used in the prompt of CLI commands:
  - Use Default—The default hostname (System Name) of these switches is: switch 123456, where 123456 represents the last three bytes of the device MAC address in hex format.
  - User Defined—Enter the hostname. Use only letters, digits, and hyphens. Host names cannot begin or end with a hyphen. No other symbols, punctuation characters, or blank spaces are permitted (as specified in RFC1033, 1034, 1035).

Step 4 Click **Next**.

Step 5 Enter the fields in the IP Settings tab:

- Interface—Select the IP interface for the system.
- IP Interface Source—Select one of the following options:
  - DHCP—Select for the device to receive its IP address from a DHCP server.

- Static—Select to enter the IP address of the device manually.

- If you selected Static as the IP interface source, enter the following fields:
  - IP Address—IP address of the interface.
  - Network Mask—IP mask for this address.
  - Administrative Default Gateway—Enter the default gateway IP address.

- DNS Server—Enter the IP address of the DNS server.

Step 6 Click **Next**

Step 7 Enter the fields in the User Account tab:

- Username—Enter a new user name between 0 and 20 characters. UTF-8 characters are not permitted.
- Password—Enter a password (UTF-8 characters are not permitted).
- Confirm Password—Enter the password again.
- Password Strength —Displays the strength of password.
- Keep current username and password—Select to keep current username and password.

Step 8 Click **Next**

Step 9 Enter the fields in the Time Settings tab:

- Clock Source—Select one of the following:
  - Manual Settings—Select to enter the device system time. If this is selected, enter the Date and Time.
  - Default SNTP Servers—Select to use the default SNTP servers.

    Note
    The default SNTP servers are defined by name, thus DNS must be configured and operational.

  - Manual SNTP Server—Select and enter the IP address of an SNTP server.

Step 10 Click **Next** to view a summary of configuration that you entered.

Step 11 Click **Apply** to save the configuration data.

VLAN Configuration Wizard

The VLAN Configuration Wizard will assist you in configuring the VLANs. Each time you run this wizard, you can configure the port memberships in a single VLAN. To use the VLAN Configuration Wizard to configure your VLANs follow these steps:

Procedure

Step 1 In **Configuration Wizards** > **VLAN Configuration Wizard**, click **Launch Wizard**.

Step 2 Click **Launch Wizard** and Next.

Step 3 Select the ports that are to be configured as trunk port (by clicking with mouse on the required ports in the graphical display). Ports that are already configured as Trunk ports are pre-selected.

Step 4 Click **Next**.

Step 5 In the VLAN Configuration section, configure the following::

- VLAN ID—Select the VLAN you want to configure. You can select either an existing VLAN or New VLAN.
- New VLAN ID—Enter the VLAN ID of a new VLAN.
- VLAN Name—Optionally, enter VLAN name.

Step 6 Select the trunk ports that are to be configured as untagged members of the VLAN (by clicking with mouse on the required ports in the graphical display). The trunk ports that are not selected in this step becomes tagged members of the VLAN.

Step 7 Click **Next**.

Step 8 Select the ports are that to be the access ports of the VLAN. Access ports of a VLAN is untagged member of the VLAN. (by clicking with mouse on the required ports in the graphical display).

Step 9 Click **Next** to see the summary of the information that you entered.

Step 10 Click **Apply**.

ACL Configuration Wizard

The ACL Configuration Wizard will assist you when creating a new ACL, or editing an existing ACL. To add or modify an existing ACL, complete the following steps:

Procedure

Step 1 In **Configuration Wizards** > **ACL Configuration Wizard**, click **Launch Wizard.**

Step 2 To create a new ACL, click **Next**. To edit an existing ACL, choose it from the ACL drop-down list and then click **Next**.

Step 3 Enter the fields:

- ACL Name—Enter the name of a new ACL.
- ACL Type—Select the type of ACL: IPv4 or MAC.

Step 4 For the ACE Configuration, configure the following fields:

- Action on match—Select one of the options:
  - Permit Traffic—Forward packets that meet the ACL criteria.

- Deny Traffic—Drop packets that meet the ACL criteria.
- Shutdown Interface—Drop packets that meet the ACL criteria, and disable the port from where the packets received.

Step 5 For a MAC-based ACL, enter the fields:

Source MAC Address	Select Any if all source address are acceptable or User defined to enter a source address or range of source addresses.
Source MAC Value	Enter the MAC address to which the source MAC address is to be matched and its mask (if relevant).
Source MAC Wildcard Mask	Enter the mask to define a range of MAC addresses.
Destination MAC Address	Select Any if all destination addresses are acceptable or User defined to enter a destination address or a range of destination addresses.
Destination MAC Value	Enter the MAC address to which the destination MAC address is to be matched and its mask (if relevant).
Destination MAC Wildcard Mask	Enter the mask to define a range of MAC addresses. Note that this mask is different than in other uses, such as subnet mask. Here, setting a bit as 1 indicates don't care and 0 indicates to mask that value. **Note** Given a mask of 0000 0000 0000 0000 0000 0000 1111 1111 (which means that you match on the bits where there is 0 and don't match on the bits where there is 1's). You need to translate the 1's to a decimal integer and you write 0 for each four zeros. In this example since 1111 1111 = 255, the mask would be written: as 0.0.0.255.
Time Range Name	If Time Range is selected, select the time range to be used.

Step 6 For a IPv4-based ACL, enter the fields:

Protocol	Select one of the following options to create an ACL based on a specific protocol: • Any (IP)—Accept all IP protocols packets • TCP—Accept Transmission Control Protocols packets • UDP—Accept User Datagram Protocols packets • ICMP—Accept ICMP Protocols packets • IGMP—Accept IGMP Protocols packets
Source Port for TCP/UDP	Select a port from the drop-down list.
Destination Port for TCP/UDP	Select a port from the drop-down list.
Source IP Address	Select Any if all source address are acceptable or User defined to enter a source address or range of source addresses.

Source IP Value	Enter the IP address to which the source IP address is to be matched.
Source IP Wildcard Mask	Enter the mask to define a range of IP addresses. Note that this mask is different than in other uses, such as subnet mask. Here, setting a bit as 1 indicates don't care and 0 indicates to mask that value.
Destination IP Address	Select Any if all IP address are acceptable or User defined to enter a destination IP address or range of destination IP addresses.
Destination IP Value	Enter the IP value to which the destination IP value is to be matched.
Destination IP Wildcard Mask	Enter the mask to define a range of IP addresses. Note that this mask is different than in other uses, such as subnet mask. Here, setting a bit as 1 indicates don't care and 0 indicates to mask that value.
Time Range Name	If Time Range is selected, select the time range to be used.

Step 7 Click **Next**.

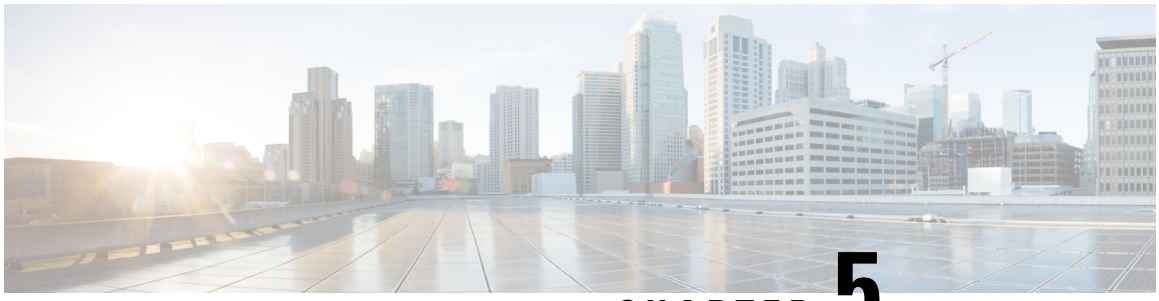
Step 8 Confirm that you want the ACL and ACE to be created.

The details of the ACL rule are displayed. You can click **Add another rule to this ACL** to add another rule.

Step 9 Click **Next** and enter the ACL Binding information:

- Binding Type—Select one of the following options to bind the ACL:
  - Physical interfaces only—Bind the ACL to a port. In this case, click a port or ports on which to bind the ACL.
  - VLANs only—Bind the ACL to a VLAN. Enter the list of VLANs in the Enter the list of VLANs you want to bind the ACL to field.
  - No binding—Do not bind the ACL.

Click **Apply**.



CHAPTER 5

Search

This chapter contains the following section:

- Search , on page 31

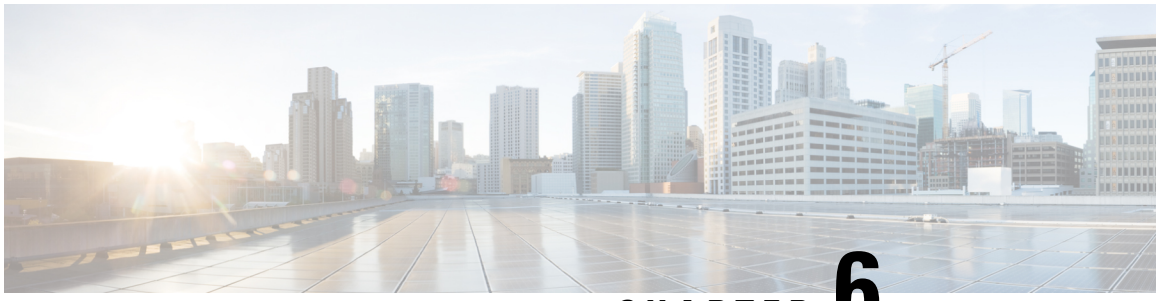
Search

The search function helps the user to locate relevant GUI pages.

The search result for a keyword includes links to the relevant pages, and also links to the relevant help pages.

To access the search function, enter a key word and click on the magnifying glass icon.

Search



CHAPTER 6

Status and Statistics

This chapter contains the following sections:

- System Summary, on page 33
- CPU Utilization, on page 35
- Port Utilization, on page 36
- Interface, on page 36
- Etherlike, on page 37
- GVRP, on page 38
- 802.1X EAP, on page 39
- ACL, on page 40
- Hardware Resource Utilization, on page 41
- Health and Power, on page 42
- SPAN and RSPAN , on page 44
- Diagnostics, on page 46
- RMON, on page 49
- sFlow, on page 54
- View Log, on page 56

System Summary

The System Summary provides a preview of the device status, hardware, firmware version, general PoE status, and other system information.

To view the system information, click **Status and Statistics** > **System Summary**.

System Information

The System Information section provides a quick way to get information about your device. In this section, you will be able to see the following information:

- System Description—A description of the system.
- System Location—Physical location of the device. Click **Edit** to go System Settings, on page 59 to enter this value.

- System Contact—Name of a contact person. Click **Edit** to go System Settings, on page 59 to enter this value.
- Host Name—Name of the device. Click **Edit** to go System Settings, on page 59 to enter this value. By default, the device host name is composed of the word switch concatenated with the three least significant bytes of the device MAC address (the six furthest right hexadecimal digits).
- System Object ID—Unique vendor identification of the network management subsystem contained in the entity (used in SNMP).
- System Uptime—Time that has elapsed since the last reboot.

Note For the System Uptime, the time counter will reset after 497 days.

- Current Time—Current system time.
- Base MAC Address—Device MAC address.
- Jumbo Frames—Jumbo frame support status. This support can be enabled or disabled by using the Port Settings, on page 119.

Note Jumbo frames support takes effect only after it is enabled, and after the device is rebooted.

Software Information

The Software Information section provides a quick way get information on the software running on your device. In this section, you will be able to see the following:

- Firmware Version (Active Image)—Firmware version number of the active image.
- Firmware MD5 Checksum (Active Image)—MD5 checksum of the active image.
- Firmware Version (Non-active)—Firmware version number of the non-active image. If the system is in a stack, the version of the active unit is displayed.
- Firmware MD5 Checksum (Non-active)—MD5 checksum of the non-active image.

TCP/UDP Services Status

To reset the following fields, click **Edit**. The following settings will be displayed.

- HTTP Service—Whether HTTP is enabled/disabled.
- HTTPS Service—Whether HTTPS is enabled/disabled.
- SNMP Service—Whether SNMP is enabled/disabled.
- Telnet Service—Whether Telnet is enabled/disabled.

- SSH Service—Whether SSH is enabled/disabled.

PoE Power Information on Device Supporting PoE

The PoE Power Information on Device Supporting PoE section provides a quick way to get PoE information on your device. In this section, the following will be displayed:

- PoE Power Information—Click on Detail to link you directly to the Properties, on page 131. This page shows the PoE power information.
- Maximum Available PoE Power (W)—Maximum available power that can be delivered by the switch.
- Total PoE Power Allocated (W)—Total PoE power allocated to connected PoE devices.
- PoE Power Mode—Port Limit or Class Limit.

The unit is displayed graphically, and hovering on a port displays its name.

The following information is displayed for each unit:

- Unit 1 (Active)—Device model ID.
- Serial Number—Serial number.

CPU Utilization

The device CPU handles the following types of traffic, in addition to end-user traffic handling the management interface:

- Management traffic
- Protocol traffic
- Snooping traffic

Excessive traffic burdens the CPU and might prevent normal device operation. The device uses the Secure Core Technology (SCT) to ensure that the device receives and processes management and protocol traffic. SCT is enabled by default on the device and can’t be disabled.

To display CPU utilization, follow these steps:

Procedure

Step 1 Click **Status and Statistics** > **CPU Utilization**.

The CPU Input Rate field displays the rate of input frames to the CPU per second. The window contains a graph displaying CPU utilization on the device. The Y axis is percentage of usage, and the X axis is the sample number.

Step 2 Check **Enable** to enable the CPU Utilization.

Step 3 Select the Refresh Rate (time period in seconds) that passes before the statistics are refreshed. A new sample is created for each time period.

The window containing a graph displaying CPU utilization on the device is displayed.

Port Utilization

The Port Utilization page displays utilization of broadband (both incoming and outgoing) per port.

To display port utilization, follow these steps:

Procedure

Step 1 Click **Status and Statistics** > **Port Utilization**.

Step 2 Enter the **Refresh Rate**, which is the time period that passes before the interface Ethernet statistics are refreshed.

The following fields are displayed for each port:

- Interface—Name of port.
- Tx Utilization—Amount of bandwidth used by outgoing packets.
- Rx Utilization—Amount of bandwidth used by incoming packets.

To view a graph of historical utilization over time on the port, select a port and click **View Interface History Graph**. In addition to the above, the following field is displayed:

- Time Span—Select a unit of time. The graph displays the port utilization over this unit of time.

Interface

The Interface page displays traffic statistics per port. This page is useful for analyzing the amount of traffic that is both sent and received, and its dispersion (Unicast, Multicast, and Broadcast).

To display Ethernet statistics and/or set the refresh rate, follow these steps:

Procedure

Step 1 Click **Status and Statistics** > **Interface**.

Step 2 To view statistics counters in table view or graphic view:

- Click **Clear Interface Counters**, to clear all counters.
- Click **Refresh** to refresh the counters.
- Click **View All Interfaces Statistics** to see all ports in table view.
- Click **View Interface History Graph** to display these results in graphic form. Select the **Interface** to view the the statistics pertaining to that interface.

Step 3 Enter the parameters.

- Interface—Select the interface for which Ethernet statistics are to be displayed.
- Refresh Rate—Select the time period that passes before the interface Ethernet statistics are refreshed.

Step 4 In the Receive Statistics section, the following stats are displayed:

- Total Bytes (Octets)—Octets received, including bad packets and FCS octets, but excluding framing bits.
- Unicast Packets—Good Unicast packets received.
- Multicast Packets—Good Multicast packets received.
- Broadcast Packets—Good Broadcast packets received.
- Packets with Errors—Packets with errors received.

Step 5 In the Transmit Statistics section, the following stats are displayed:

- Total Bytes (Octets)—Octets transmitted, including bad packets and FCS octets, but excluding framing bits.
- Unicast Packets—Good Unicast packets transmitted.
- Multicast Packets—Good Multicast packets transmitted.
- Broadcast Packets—Good Broadcast packets transmitted.

Etherlike

The Etherlike page displays statistics per port according to the Etherlike MIB standard definition. The refresh rate of the information can be selected. This page provides more detailed information regarding errors in the physical layer (Layer 1) that might disrupt traffic.

To view Etherlike Statistics and/or set the refresh rate follow these steps:

Procedure

Step 1 Click **Status and Statistics** > **Etherlike**.

Step 2 Enter the parameters.

- Interface-Select the specific interface for which Ethernet statistics are to be displayed.
- Refresh Rate-Select the amount of time that passes before the Etherlike statistics are refreshed.

The fields are displayed for the selected interface.

- Frame Check Sequence (FCS) Errors- Received frames that failed the CRC (cyclic redundancy checks).
- Single Collision Frames- Frames that involved in a single collision, but successfully transmitted.
- Late Collisions- Collisions that have been detected after the first 512 bits of data.

- Excessive Collisions- Transmissions rejected due to excessive collisions.
- Oversize Packets- Packets greater than 2000 octets received.
- Internal MAC Receive Errors- Frames rejected because of receiver errors.
- Pause Frames Received- Displays the number of frames received.
- Pause Frames Transmitted- Number of pause frames transmitted.

Note
If one of the fields listed above shows a number of errors (not 0), a Last Up time is displayed.

Step 3 To view statistics counters in table view, click **View All Interfaces Statistics** to see all ports in table view. You can also click **Refresh** to refresh the stats or click **Clear Interface Counters** to clear the counters.

GVRP

The GARP VLAN Registration Protocol (GVRP) page displays the GVRP frames that are sent or received from a port. GVRP is a standards-based Layer 2 network protocol, for automatic configuration of VLAN information on switches. It is defined in the 802.1ak amendment to 802.1Q-2005. GVRP statistics for a port are only displayed if GVRP is enabled globally and on the port.

To view GVRP statistics and/or set the refresh rate, proceed as follows:

Procedure

Step 1 Click **Status and Statistics** > **GVRP**.

Step 2 Enter the parameters.

Interface	Select the specific interface for which GVRP statistics are to be displayed.
Refresh Rate	Select the time period that passes before the GVRP page is refreshed. The Attribute Counter block displays the counters for various types of packets per interface. These are displayed for Received and Transmitted packets.

Received - Transmitted

Join Empty	GVRP Join Empty packets received/transmitted.
Empty	GVRP empty packets received/transmitted
Leave Empty	GVRP Leave Empty packets received/transmitted.
Join In	GVRP Join In packets received/transmitted.
Leave In	GVRP Leave In packets received/transmitted.
Leave All	GVRP Leave All packets received/transmitted. The GVRP Error Statistics section displays the GVRP error counters.

GVRP Error Statistics

Invalid Protocol ID	Invalid protocol ID errors.
Invalid Attribute Type	Invalid attribute ID errors.
Invalid Attribute Value	Invalid attribute value errors.
Invalid Attribute Length	Invalid attribute length errors.
Invalid Event	Invalid events.

Step 3 To clear statistics counters, click **Clear Interface Counters.**

Step 4 To view all interface statistics, click **View All Interfaces Statistics** to see all ports on a single page.

802.1X EAP

The 802.1x EAP page displays the Extensible Authentication Protocol (EAP) frames that are sent or received. To view the EAP Statistics and/or set the refresh rate, proceed as follows:

Procedure

Step 1 Click **Status and Statistics** > **802.1x EAP**.

Step 2 Select the Interface that is polled for statistics.

Step 3 Select the Refresh Rate (time period) that passes before the EAP statistics are refreshed.

The values are displayed for the selected interface.

EAPOL EAP Frames Received	Valid EAPOL frames received on the port.
EAPOL Start Frames Received	Valid EAPOL start frames received on the port.
EAPOL Logoff Frames Received	EAPOL Logoff frames received on the port.
EAPOL Announcement Frames Received	EAPOL Announcement frames received on the port.
EAPOL Announcement Request Frames Received	EAPOL Announcement Request frames received on the port.
EAPOL Invalid Frames Received	EAPOL invalid frames received on the port.
EAPOL EAP Length Error Frames Received	EAPOL frames with an invalid Packet Body Length received on this port.
MKPDU Frames with unrecognized CKN Received	EAP frames with unrecognized CKN received on this port.
MKPDU Invalid Frames Received	MKPDU invalid frames received on the port.

Last EAPOL Frame Version	Protocol version number attached to the most recently received EAPOL frame.
Last EAPOL Frame Source	Source MAC address attached to the most recently received EAPOL frame.
EAPOL EAP Supplicant Frames Transmitted	EAPOL EAP Supplicant frames transmitted on the port.
EAPOL Start Frames Transmitted	EAPOL Start frames transmitted on the port.
EAPOL Logoff Frames Transmitted	EAPOL Logoff frames transmitted on the port.
EAPOL Announcement Frames Transmitted	EAPOL Announcement frames transmitted on the port.
EAPOL Announcement Request Frames Transmitted	EAPOL Announcement Request frames transmitted on the port.
EAPOL EAP Authenticator Frames Transmitted	EAP Authenticator frames transmitted on the port.
EAPOL MKA Frames with No CKN Transmitted	MKA frames with no CKN transmitted on the port.

Step 4 To clear statistics counters:

- Click **Clear Interface Counters** to clear the counters of all interfaces.
- Click **Refresh** to refresh the counters.
- Click **View All Interfaces Statistics** to view the counters of all interfaces.

ACL

When the ACL logging feature is enabled, an informational SYSLOG message is generated for packets that match ACL rules. To view the interfaces on which packets are forwarded or rejected based on ACLs, follow these steps:

Procedure

Step 1 Click **Status and Statistics** > **ACL**.

Step 2 Select the Refresh Rate (time period in seconds) that passes before the page is refreshed. A new group of interfaces is created for each time period.

The following information is displayed:

- Global Trapped Packet Counter—Number of packets trapped globally due to lack of resources.
- Trapped Packets - Port/LAG Based—The interfaces on which packets forwarded or rejected based on ACL rules.
- Trapped Packets - VLAN Based—The VLANs on which packets forwarded or rejected based on ACL rules.

Step 3 To clear statistics counters, click **Clear Counters** or click **Refresh** to refresh the counters.

Hardware Resource Utilization

This page displays the resources used by the device, such as Access Control Lists (ACL) and Quality of Service (QoS). Some applications allocate rules upon their initiation. Also, processes that initialize during the system boot use some of their rules during the startup process.

To view the hardware resource utilization, click **Status and Statistics** > **Hardware Resource Utilization**.

The following fields are displayed:

- Unit No—Unit in stack for which TCAM utilization appears. This is not displayed when the device is in not part of a stack.
- IP Entries
  - In Use—Number of TCAM entries used for IP rules.
  - Maximum—Number of available TCAM entries that can be used for IP rules.
- IPv4 Policy Based Routing
  - In Use—Number of router TCAM entries used for IPv4 Policy-based routing
  - Maximum—Maximum number of available router TCAM entries that can be used for IPv4 Policy-based routing.
- IPv6 Policy Based Routing
  - In Use—Number of router TCAM entries used for IPv6 Policy-based routing
  - Maximum—Maximum number of available router TCAM entries that can be used for IPv6 Policy-based routing.
- VLAN Mapping
  - In Use—Number of router TCAM entries currently used for VLAN mapping
  - Maximum—Maximum number of available router TCAM entries that can be used for VLAN mapping.
- ACL and QoS Rules
  - In Use—Number of TCAM entries used for ACL and QoS rules
  - Maximum—Number of available TCAM entries that can be used for ACL and QoS rules.

To view the hardware resources, click the **Hardware Resources Management** button.

The following fields are displayed:

- Maximum IPv4 Policy-Based Routes
  - Use Default—Use default values.

- User Defined—Enter a user defined value (Range 0-32, Default 12).

- Maximum IPv6 Policy-Based Routes
  - Use Default—Use default values.
  - User Defined—Enter a user defined value (Range 0-32, Default 12).

- (Range 0-32, Default 12)
- Maximum VLAN-Mapping Entries
  - Use Default—Use default values.
  - User Defined—Enter a user defined value (Range 0-228, Default 0).

- Hardware-Based Routing: Displays whether hardware-based routing is active or inactive.

Health and Power

The Health and Power page monitors the temperature, power supply, and fan status on all relevant devices. The fans on the device vary based on the model.

To view the settings on the Heath and Power page, navigate to **Status and Statistics > Heath and Power**.

Environmental Status

- Fan Status—Displays whether the fan is not available (N/A) or is available and is operating normally (OK) or not (Failure).
- Sensor Status—Displays whether the sensor is functional (OK) or not functional (Failure).
- Temperature—Displays one of the following options:
  - OK—The temperature is below the warning threshold.
  - Warning—The temperature is between the warning threshold to the critical threshold.
  - Critical—Temperature is above the critical threshold.
  - N/A—Not relevant.

Main Power Status

- Main Power Supply Status— Displays the main power supply status.

Power Savings

- Current Green Ethernet and Port Power Savings—Current amount of the power savings on all the ports.
- Cumulative Green Ethernet and Port Power Savings—Accumulative amount of the power savings on all the ports since the device was powered up.

- Projected Annual Green Ethernet and Port Power Savings—Projection of the amount of the power that will be saved on the device during one week. This value is calculated based on the savings that occurred during the previous week.
- Current PoE Power Savings (available for PoE SKUs only)—Current amount of the PoE power saved on ports that have PDs connected to them and on which PoE is not operational due to the Time Range feature.
- Cumulative PoE Power Savings (available for PoE SKUs only)—Cumulative amount of the PoE power, since the device was powered up, saved on ports which have PDs connected to them and to which PoE is not operational due to the Time Range feature.
- Projected Annual PoE Power Savings (available for PoE SKUs only)—Yearly projected amount of PoE power, since device was powered up, saved on ports that have PDs connected to them and to which PoE is not operational due to the Time Range feature. The projection is based on the savings during the previous week.

Health Table

- Unit No.—Displays the unit number in the stack.
- Fan Status— Displays the status of the fan.
  - OK—Fan is operating normally.
  - Failure—A fan is not operating correctly.
  - N/A—Fan is not applicable for the specific model.
- Redundant Fan Status— Displays the redundant status of the fan:
  - N/A—Redundant fan is not applicable for the specific model.
  - Ready—Redundant fan is operational but not required.
  - Active—One of the main fans is not working and this fan is replacing it.



Note The Redundant Fan Status is only supported on certain SKUs.

- Sensor Status—The following values are possible:
  - OK—Sensor is functional.
  - Failure—Sensor has a failure.
- Temperature—The options are:
  - OK—The temperature is below the warning threshold.
  - Warning—The temperature is between the warning threshold to the critical threshold.
  - Critical—Temperature is above the critical threshold.
  - N/A—Not relevant.

SPAN and RSPAN

The SPAN feature, which is sometimes called port mirroring or port monitoring, selects network traffic for analysis by a network analyzer. The network analyzer can be a Cisco Switch Probe device or other Remote Monitoring (RMON) probes.

Port mirroring is used on a network device to send a copy of network packets, seen on a single device port, multiple device ports, or an entire VLAN, to a network monitoring connection on another port on the device. This is commonly used when monitoring of network traffic, such as for an intrusion-detection system, is required. A network analyzer, connected to the monitoring port, processes the data packets. A packet, which is received on a network port and assigned to a VLAN that is subject to mirroring, is mirrored to the analyzer port even if the packet was eventually trapped or discarded. Packets sent by the device are mirrored when Transmit (Tx) mirroring is activated.

Mirroring does not guarantee that all traffic from the source port(s) is received on the analyzer (destination) port. If more data is sent to the analyzer port than it can support, some data might be lost.

VLAN mirroring cannot be active on a VLAN that was not manually created. For example, if VLAN 23 was created by GVRP, port mirroring will not work on it.

RSPAN

RSPAN extends SPAN by enabling monitoring of multiple switches across your network and allowing the analyzer port to be defined on a remote switch. In addition to the start (source) and final (destination) switches, you can define intermediate switches over which the traffic flows. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The traffic from the source interfaces on the start device is copied to the RSPAN VLAN through a reflector port and then forwarded over trunk ports configured in general mode on the intermediate devices to the destination session on the final switch, which is monitoring the RSPAN VLAN. The reflector port is the mechanism that copies packets to an RSPAN VLAN. It is a network port that handles various types of traffic. The RSPAN VLAN must be configured on all the intermediate switches.

RSPAN VLAN

An RSPAN VLAN carries SPAN traffic between RSPAN source and destination sessions and must be defined on the start, intermediate and final devices.

Note A VLAN must be added to the VLAN Database using the VLAN Settings, on page 143 screen before it can be configured as an RSPAN VLAN.

To configure a VLAN as an RSPAN VLAN, follow these steps:

Procedure

Step 1 Click **Status and Statistics** > **SPAN & RSPAN** > **RSPAN VLAN.** to view the previously defined RSPAN VLAN.

Step 2 To configure a VLAN as a RSPAN VLAN, select it from the RSPAN VLAN drop-down list of VLANs.

Step 3 Click **Apply**.

SPAN Session Destinations

A monitoring session consists of one or more source ports and a single destination ports. A destination port must be configured on the start and final devices. On the start device, this is the reflector port. On the final device, it is the analyzer port.

To add a destination port, follow these steps:

Procedure

Step 1 Click **Status and Statistics >SPAN & RSPAN> SPAN Session Destinations**.

Step 2 Click **Add**.

Step 3 Enter the following fields:

- Session ID—Select a session ID. This must match the session IDs of the source ports.
- Port—Select a port from the drop-down list.
- Destination Type—Select one of the following options:
  - Local Interface—Is the destination port on the same device as the source ports (relevant to SPAN).
  - Remote VLAN—Is the destination port on a different device than the source port (relevant to RSPAN).

  If the Destination Type is Remote VLAN, configure the following field:
  - Reflector Port—Select a unit/port that functions as a target port on the first device.

  If the Destination Type is Local Interface, configure the following field:
- Network Traffic—Select to enable that traffic other than monitored traffic is possible on the port.

Step 4 Click **Apply**.

SPAN Session Sources

In a single local SPAN or RSPAN session source, you can monitor the port traffic, such as received (Rx), transmitted (Tx), or bidirectional (both). The switch supports up to 8source ports per session ID.

Note One or more SPAN or RSPAN sources must be configured on the start and final devices.

To configure the source ports to be mirrored, follow these steps:

Procedure

Step 1 Click **Status and Statistics** > **SPAN and RSPAN** > **SPAN Session Sources**.

Step 2 Click **Add**.

Step 3 Select the session number from Session ID. This must be the same for all source ports and the destination port.

Step 4 For SPAN or for RSPAN on the start switch, select the unit and port or VLAN from which traffic is monitored (Source Interface). On the final switch, for RSPAN, select Remote VLAN

Step 5 In the **Monitor Type** field, select whether incoming, outgoing, or both types of traffic are mirrored.

- Rx and Tx—Port mirroring on both incoming and outgoing packets
- Rx—Port mirroring on incoming packets
- Tx—Port mirroring on outgoing packets

Step 6 Click **Apply**. The source interface for the mirroring is configured.

Diagnostics

You can use diagnostics to test and verify the functionality of the hardware components of your system (chassis, supervisor engines, modules, and ASICs) while your device is connected to a live network. Diagnostics consists of packet-switching tests that test hardware components and verify the data path and control signals.

Copper Test

The Copper Test page displays the results of integrated cable tests performed on copper cables by the Virtual Cable Tester (VCT).

VCT performs two types of tests:

- Time Domain Reflectometry (TDR) technology tests the quality and characteristics of a copper cable attached to a port. Cables of up to 140 meters long can be tested. These results are displayed in the Test Results block of the Copper Test page.
- DSP-based tests are performed on active XG links to measure cable length. These results are displayed in the Advanced Information block of the Copper Test page. This test can run only when the link speed is 10G.

Preconditions to Running the Copper Test

Before running the test, do the following:

- (Mandatory) Disable Short Reach mode (see Properties, on page 136).
- (Optional) Disable EEE (see Properties, on page 136).

Use a CAT6a data cable when testing cables using (VCT).

The test results have an accuracy within an error range of +/- 10 for advanced Testing and +/-2 for basic testing.

Caution When a port is tested, it is set to the Down state and communications are interrupted. After the test, the port returns to the Up state. It is not recommended that you run the copper port test on a port you are using to run the web-based switch configuration utility, because communications with that device are disrupted.

To test copper cables attached to ports:, follow these steps

Procedure

Step 1 Click **Status and Statistics > Diagnostics > Copper Test**.

Step 2 Select the unit and port on which to run the test.

Step 3 Click **Copper Test**.

Step 4 When the message appears, click **OK** to confirm that the link can go down or **Cancel** to abort the test. The following fields are displayed in the Test Results block:

- Last Update—Time of the last test conducted on the port
- Test Results—Cable test results. Possible values are:
  - OK—Cable passed the test.
  - No Cable—Cable is not connected to the port.
  - Open Cable—Cable is connected on only one side.
  - Short Cable—Short circuit has occurred in the cable.
  - Unknown Test Result—Error has occurred.
- Distance to Fault—Distance from the port to the location on the cable where the fault was discovered.
- Operational Port Status—Displays whether port is up or down.

The Advanced Information block (supported on some of the port types) contains the following information, which is refreshed each time you enter the page:

- Cable Length—Provides an estimate for the length.
- Pair—Cable wire pair being tested.
- Status—Wire pair status. Red indicates fault and Green indicates status OK.
- Channel—Cable channel indicating whether the wires are straight or cross-over.
- Polarity—Indicates if automatic polarity detection and correction has been activated for the wire pair.
- Pair Skew—Difference in delay between wire pairs.

Optical Module Status

The Optical Module Status page displays the operating conditions reported by the SFP (Small Form-factor Pluggable) transceiver.

The following GE SFP (1000Mbps) transceivers are supported:

- MGBLH1: 1000BASE-LH SFP transceiver, for single-mode fiber, 1310 nm wavelength, supports up to 40 km.
- MGBLX1: 1000BASE-LX SFP transceiver, for single-mode fiber, 1310 nm wavelength, supports up to 10 km.
- MGBSX1:1000BASE-SX SFP transceiver, for multimode fiber, 850 nm wavelength, supports up to 550 m.
- MGBT1: 1000BASE-T SFP transceiver for category 5 copper wire, supports up to 100 m.
- GLC-SX-MMD - 1000BASE-SX short wavelength; with DOM
- GLC-LH-SMD - 1000BASE-LX/LH long-wavelength; with DOM
- GLC-BX-D - 1000BASE-BX10-D downstream bidirectional single fiber; with DOM
- GLC-BX-U - 1000BASE-BX10-U upstream bidirectional single fiber; with DOM
- GLC-TE - 1000BASE-T standard

The following XG SFP+ (10,000Mbps) transceivers are supported:

- Cisco SFP-10GBase-T
- Cisco SFP-10G-SR
- Cisco SFP-10G-LR
- Cisco SFP-10G-SR-S
- Cisco SFP-10G-LR-S

The following XG passive cables (Twinax/DAC) are supported:

- Cisco SFP-H10G-CU1M
- Cisco SFP-H10G-CU3M
- Cisco SFP-H10G-CU5M

To view the results of optical tests, click **Status and Statistics** > **Diagnostics** > **Optical Module Status**.

This page displays the following fields:

- Port—Port number on which the SFP is connected
- Description—Description of optical transceiver
- Serial Number—Serial number of optical transceiver
- PID—Product ID of the transceiver
- VID—Version ID of the transceiver

- Temperature—Temperature (Celsius) at which the SFP is operating
- Voltage—SFPs operating voltage
- Current—SFPs current consumption
- Output Power—Transmitted optical power
- Input Power—Received optical power
- Transmitter Fault—Remote SFP reports signal loss. Values are True, False, and No Signal (N/S)
- Loss of Signal—Local SFP reports signal loss. Values are True and False
- Data Ready—SFP is operational. Values are True and False

Tech-Support Information

This page provides a detailed log of the device status. This is valuable when the technical support is trying to help a user with a problem, since it gives the output of many show commands (including debug command) in a single command.

To view technical support information useful for debugging purposes:

Procedure

Step 1 Click **Status and Statistics** > **Diagnostics** > **Tech-Support Information**.

Step 2 Click **Generate**.

Note
Generation of output from this command may take some time. When the information is generated, you can copy it from the text box in the screen by clicking on **Select tech-support data**.

RMON

Remote Networking Monitoring (RMON) enables an SNMP agent in the device to proactively monitor traffic statistics over a given period and send traps to an SNMP manager. The local SNMP agent compares actual, real-time counters against predefined thresholds and generates alarms, without the need for polling by a central SNMP management platform. This is an effective mechanism for proactive management, provided that you have set the correct thresholds relative to your network's base line.

RMON decreases the traffic between the manager and the device since the SNMP manager does not have to poll the device frequently for information, and enables the manager to get timely status reports, since the device reports events as they occur.

With this feature, you can perform the following actions:

- View the current statistics (from the time that the counter values cleared). You can also collect the values of these counters over a period of time, and then view the table of collected data, where each collected set is a single line of the History tab.
- Define interesting changes in counter values, such as “reached a certain number of late collisions” (defines the alarm), and then specify what action to perform when this event occurs (log, trap, or log and trap).

Statistics

The Statistics page displays detailed information regarding packet sizes and information regarding physical layer errors. The information is displayed according to the RMON standard. An oversized packet is defined as an Ethernet frame with the following criteria:

- Packet length is greater than MRU byte size.
- Collision event has not been detected.
- Late collision event has not been detected.
- Received (Rx) error event has not been detected.
- Packet has a valid CRC.

To view RMON statistics and/or set the refresh rate, complete the following:

Procedure

Step 1 Click **Status and Statistics** > **RMON** > **Statistics**.

Step 2 Select the Interface for which Ethernet statistics are to be displayed.

Step 3 Select the Refresh Rate, which is the time period that passes before the interface statistics are refreshed.

The following statistics are displayed for the selected interface.

Bytes Received	Octets received, including bad packets and FCS octets, but excluding framing bits.
Drop Events	Packets dropped.
Packets Received	Good packets received including Multicast and Broadcast packets.
Broadcast Packets Received	Good Broadcast packets received. This number does not include Multicast packets.
Multicast Packets Received	Good Multicast packets received.
CRC & Align Errors	CRC and Align errors that have occurred.
Undersize Packets	Undersized packets (less than 64 octets) received.
Oversize Packets	Oversized packets (over 2000 octets) received.
Fragments	Fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.

Jabbers	Received packets that are longer than 1632 octets. This number excludes frame bits, but includes FCS octets that had either a bad FCS (Frame Check Sequence) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. A Jabber packet is defined as an Ethernet frame that satisfies the following criteria:
Collisions	Collisions received. If Jumbo frames are enabled, the threshold of Jabber frames is raised to the maximum size of Jumbo frames.
Frames of 64 Bytes	Frames, containing 64 bytes that were sent or received.
Frames of 65 to 127 Bytes	Frames, containing 65-127 bytes that were sent or received.
Frames of 128 to 255 Bytes	Frames, containing 128-255 bytes that were sent or received.
Frames of 256 to 511 Bytes	Frames, containing 256-511 bytes that were sent or received.
Frames of 512 to 1023 Bytes	Frames, containing 512-1023 bytes that were sent or received.
Frames of 1024 Bytes or More	Frames, containing 1024-2000 bytes, and Jumbo Frames, that were sent or received.

Note
If one of the fields above shows a number of errors (not 0), a Last Update time is displayed.

Step 4 To view counters in table view or graphic view:

- Click **View All Interfaces Statistics** to see all ports in table view.
- Click **Graphic View** to display these results in graphic form. In this view, you can select the Time Span for which the results will be displayed and the type of statistic to be displayed.

History

The RMON feature enables monitoring statistics per interface.

The History page defines the sampling frequency, amount of samples to store and the port from which to gather the data. After the data is sampled and stored, it appears in the History Table page that can be viewed by clicking History Table.

To enter RMON control information, complete the following:

Procedure

Step 1 Click **Status and Statistics** > **RMON** > **History**. The fields displayed on this page are defined in the Add RMON History page, below. The only field is that is on this page and not defined in the Add page is:

- Current Number of Samples-RMON is allowed by the standard not to grant all requested samples, but rather to limit the number of samples per request. Therefore, this field represents the sample number granted to the request that is equal or less than the requested value.

Step 2 Click **Add**.

Step 3 Enter the parameters.

- New History Entry-Displays the number of the new History table entry.
- Source Interface-Select the type of interface from which the history samples are to be taken.
- Max No. of Samples to Keep-Enter the number of samples to store.
- Sampling Interval-Enter the time in seconds that samples are collected from the ports. The field range is 1-3600.
- Owner-Enter the RMON station or user that requested the RMON information.

Step 4 Click **Apply**. The entry is added to the History Control Table page, and the Running Configuration file is updated.

Step 5 Click **History Table** to view the actual statistics.

Events

You can control the occurrences that trigger an alarm and the type of notification that occurs. This is performed as follows:

- Events Page—Configures what happens when an alarm is triggered. This can be any combination of logs and traps.
- Alarms Page—Configures the occurrences that trigger an alarm.

To define RMON events, complete the following steps:

Procedure

Step 1 Click **Status and Statistics** > **RMON** > **Events**.

Step 2 Click **Add.**

Step 3 Enter the parameters.

- Event Entry Number—Displays the event entry index number for the new entry.
- Community—Enter the SNMP community string to be included when traps are sent (optional).
- Description—Enter a name for the event. This name is used in the Add RMON Alarm page to attach an alarm to an event.
- Notification Type—Select the type of action that results from this event. Values are:
  - None—No action occurs when the alarm goes off.
  - Log (Event Log Table)—Add a log entry to the Event Log table when the alarm is triggered.
  - Trap (SNMP Manager and Syslog Server)—Send a trap to the remote log server when the alarm goes off.

- Log and Trap—Add a log entry to the Event Log table and send a trap to the remote log server when the alarm goes off.

- Owner—Enter the device or user that defined the event.

Step 4 Click **Apply**. The RMON event is saved to the Running Configuration file.

Step 5 Click **Event Log Table** to display the log of alarms that have occurred and that have been logged (see description below).

Alarms

RMON alarms provide a mechanism for setting thresholds and sampling intervals to generate exception events on counters or any other SNMP object counter maintained by the agent. Both the rising and falling thresholds must be configured in the alarm. After a rising threshold is crossed, no rising events are generated until the companion falling threshold is crossed. After a falling alarm is issued, the next alarm is issued when a rising threshold is crossed.

One or more alarms are bound to an event, which indicates the action to be taken when the alarm occurs.

Alarm counters can be monitored by either absolute values or changes (delta) in the counter values.

To enter RMON alarms, complete the following steps:

Procedure

Step 1 Click **Status and Statistics** > **RMON** > **Alarms**.

All previously defined alarms are displayed. The fields are described in the Add RMON Alarm page below. In addition to those fields, the following field appears:

- Counter Value—Displays the value of the statistic during the last sampling period.

Step 2 Click **Add.**

Step 3 Enter the parameters.

Alarm Entry	Displays the alarm entry number.
Interface	Select the type of interface for which RMON statistics are displayed.
Counter Name	Select the MIB variable that indicates the type of occurrence measured.
Sample Type	Select the sampling method to generate an alarm. The options are: • Absolute—If the threshold is crossed, an alarm is generated. • Delta—Subtracts the last sampled value from the current value The difference in the values is compared to the threshold. If the threshold was crossed, an alarm is generated.
Rising Threshold	Enter the value that triggers the rising threshold alarm.

Rising Event	Select an event to be performed when a rising event is triggered. Events are configured in the Events, on page 52.
Falling Threshold	Enter the value that triggers the falling threshold alarm.
Falling Event	Select an event to be performed when a falling event is triggered.
Startup Alarm	Select the first event from which to start generation of alarms. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold. • Rising Alarm—A rising value triggers the rising threshold alarm. • Falling Alarm—A falling value triggers the falling threshold alarm. • Rising and Falling—Both rising and falling values trigger the alarm.
Interval	Enter the alarm interval time in seconds.
Owner	Enter the name of the user or network management system that receives the alarm.

Step 4 Click **Apply**. The RMON alarm is saved to the Running Configuration file.

sFlow

The sFlow monitoring system consists of an sFlow agent (embedded in a switch or router or in a stand alone probe) and a central data collector, known as the sFlow collector. The sFlow agent uses sampling technology to capture traffic and statistics from the device it is monitoring. sFlow datagrams are used to forward the sampled traffic and statistics to an sFlow collector for analysis.

sFlow V5 defines:

- How traffic is monitored.
- The sFlow MIB that controls the sFlow agent.
- The format of the sample data used by the sFlow agent when forwarding data to a central data collector. The device provides support for two types of sFlow sampling: flow sampling and counters sampling. The following counters sampling is performed according to sFlow V5 (if supported by the interface):
  - Generic interface counters (RFC 2233)
  - Ethernet interface counters (RFC 2358)

sFlow Receivers

The sFlow receiver defines the set of objects used to maintain a sFlow session between a sFlow Agent and a sFlow Collector. To set the sFlow receiver parameters, follow these steps:

Procedure

Step 1 Click **Status and Statistics** > **sFlow** > **sFlow Receivers**.

Step 2 Enter the following fields:

- IPv4 Source Interface—Select the IPv4 source interface.

  Note
  If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

- IPv6 Source Interface— Select the IPv6 source interface

Step 3 To add a receiver (sFlow analyzer), click **Add** and select one of the predefined sampling definition indices in Receiver Index.

Step 4 Enter the receiver's address fields:

- Receiver Definition—Select whether to specify the sFlow server By IP address or By name.

  If Receiver Definition is By IP Address:

- IP Version—Select whether an IPv4 or an IPv6 address for the server is used.
- IPv6 Address Type—Select the IPv6 address type (if IPv6 is used). The options are:
  - Link Local —The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- Link Local Interface—Select the link local interface (if IPv6 is used) from the list.

Step 5 Enter the following fields:

- Receiver IP Address/Name—Enter the IP address or the name of the receiver, whichever is relevant.
- Port—Port to which SYSLOG messages are sent.
- Maximum Datagram Size—Maximum number of bytes that can be sent to the receiver in a single sample datagram (frame).

Step 6 Click **Apply**.

sFlow Interface Settings

To sample datagrams or counters from a port, the port must be associated with a receiver. sFlow port settings can be configured only after a receiver has been defined in the sFlow Receivers, on page 54 pages.

To enable sampling and configure the port from which to collect the sFlow information, follow these steps:

Procedure

Step 1 Click **Status and Statistics** > **sFlow** > **sFlow Interface Settings**.

The sFlow interface settings are displayed.

Step 2 To associate an sFlow receiver with a port, select a port, click **Edit**, and enter the fields:

- Interface—Select the unit/port from which information is collected.
- (Flow Sampling) State—Enable/disable flow sampling.
- Sampling Rate—If x is entered, a flow sample will be taken for each x frame.
- Maximum Header Size (Bytes)—Maximum number of bytes that should be copied from a sampled packet.
- Receiver Index—Select one of the indices that was defined in the sFlow Receivers, on page 54 pages.
- (Counter Sampling) State—Enable/disable counters sampling.
- Sampling Interval (Sec.)—If x is entered, this specifies that a counter sample will be taken for each x seconds.
- Receiver Index—Select one of the indices that was defined in these sFlow Receivers, on page 54 pages.

Step 3 Click **Apply**.

sFlow Statistics

To view the sFlow statistics, complete the following:

Procedure

Step 1 Click **Status and Statistics > sFlow > sFlow Statistics**.

Step 2 Select the Refresh Rate from the drop-down menu.

The following sFlow statistics per interface are displayed.

- Port—Port for which sample was collected.
- Packets Sampled—Number of packets sampled.
- Datagrams Sent to Receiver—Number of sFlow sampling packets sent.

View Log

The device can write to the following logs:

- Log in RAM (cleared during reboot).
- Log in Flash memory (cleared only upon user command).

You can configure the messages that are written to each log by severity, and a message can go to more than one log, including logs that reside on external SYSLOG servers.

RAM Memory

The RAM Memory page displays all messages that are saved in the RAM (cache) in chronological order. All entries are stored in the RAM log.

Pop-Up SYSLOG Notifications

When a new SYSLOG message is written to the RAM log file, a notification is displayed on the web GUI showing its contents. The web GUI polls the RAM log every 10 seconds. Syslog notifications pop-ups for all SYSLOGs created in the last 10 seconds appear at the bottom right of the screen.

If more than 7 pop-up notifications are displayed, a summary pop-up is displayed. This pop-up states how many SYSLOG notifications aren't displayed. It also contains a button that enables closing all of the displayed pop-ups.

To view log entries, click **Status and Statistics** > **View Log** > **RAM Memory**.

The following are displayed at the top of the page:

- Alert Icon Blinking—Toggles between disable and enable.
- Pop-Up Syslog Notifications—Enables receiving pop-up SYSLOGs as described above.
- Current Logging Threshold—Specifies the levels of logging that are generated. This can be changed by clicking Edit by the field's name.

This page contains the following fields for every log file:

- Log Time—Time when message was generated.
- Severity—Event severity
- Description—Message text describing the event

To clear the log messages, click **Clear Logs.**

Flash Memory

The Flash Memory page displays the messages that stored in the Flash memory, in chronological order. The minimum severity for logging is configured in the Log Settings, on page 71. Flash logs remain when the device is rebooted. You can clear the logs manually.

To view the Flash logs, click **Status and Statistics** > **View Log** > **Flash Memory**.

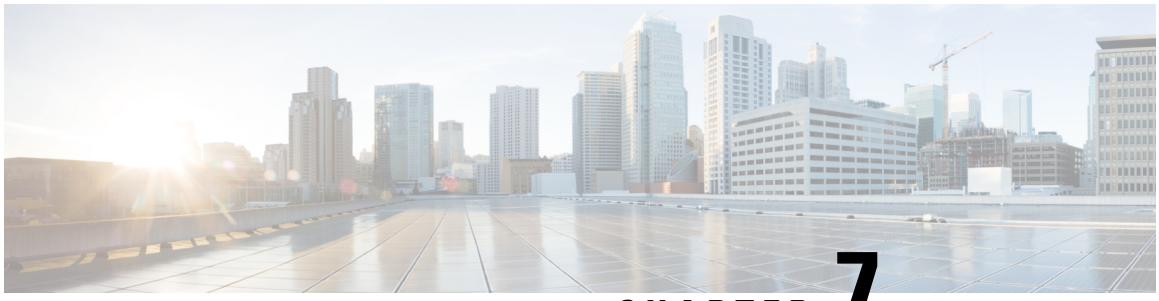
The Current Logging Threshold specifies the levels of logging that are generated. This can be changed by clicking Edit by the field's name.

This page contains the following fields for each log file:

- Log Index—Log entry number

- Log Time—Time when message was generated.
- Severity—Event severity
- Description—Message text describing the event

To clear the messages, click **Clear Logs.** The messages are cleared.



CHAPTER 7

Administration

This chapter contains the following sections:

- System Settings, on page 59
- Console Settings , on page 60
- Stack Management, on page 61
- User Accounts, on page 62
- Idle Session Timeout, on page 63
- Time Settings, on page 63
- System Log, on page 70
- File Management, on page 73
- Cisco Business Dashboard Settings, on page 81
- Plug-n-Play (PNP), on page 84
- Reboot, on page 90
- Hardware Resources, on page 91
- Discovery Bonjour, on page 92
- Discovery - LLDP, on page 92
- Discovery - CDP, on page 108
- Locate Device, on page 115
- Ping, on page 115
- Traceroute, on page 117

System Settings

The system setting page allows you customize the settings on your switch. You can configure the following:

Procedure

Step 1 Click **Administration** > **System Settings**.

Step 2 View or modify the system settings.

- System Description—Displays a description of the device.
- System Location—Enter the physical location of the device.

- System Contact—Enter the name of a contact person.
- Host Name—Select the host name of this device. This is used in the prompt of CLI commands:
  - Use Default—The default hostname (System Name) of these switches is: switch123456, where 123456 represents the last three bytes of the device MAC address in hex format.
  - User Defined—Enter the hostname. Use only letters, digits, and hyphens. Host names can't begin or end with a hyphen. No other symbols, punctuation characters, or blank spaces are permitted (as specified in RFC1033, 1034, 1035).
- Custom Banner Settings—The following banners can be set:
  - Login Banner—Enter text to display on the Login page before login. Click **Preview** to view the results.
  - Welcome Banner—Enter text to display on the Login page after login. Click **Preview** to view the results.

  Note
  When you define a login banner from the web-based configuration utility, it also activates the banner for the CLI interfaces (Console, Telnet, and SSH).

  The banner can contain up to 1000 characters. After 510 characters, press <Enter> to continue.

Step 3 Click **Apply** to save the values in the Running Configuration file.

Console Settings



Note The Console Setting is only available in the Advanced Mode view.

The console port speed can be set to one of the following speeds: 9600, 19200, 38400, 57600, and 115200 or to Auto Detection. If Auto Detection is selected, the device detects console speed automatically. When Auto Detection is not enabled, the console port speed is automatically set to the last speed that was set manually at (115,200 by default). When Auto Detection is enabled but the console baud-rate has not yet been discovered, the system uses speed 115,200 for displaying text (for example, the boot-up information). After Auto Detection is enabled in the Console Settings page, it can be activated by connecting the console to the device and pressing the Enter key twice. The device detects the baud rate automatically.

To enable Auto Detection or to manually set the baud rate of the console, follow these steps:

Procedure

Step 1 Click **Administration** > **Console Settings**.

Step 2 Select one of the following options in the Console Port Baud Rate field:

- Auto Detection—The console baud rate is detected automatically.
- Static—Select one of the available speeds.

Step 3 Click **Apply**.

Stack Management



Note Only certain models have stacking capabilities.

To manage the stack, complete the following steps:

Procedure

Step 1 Click **Administration** > **Stack Management**.

- Stack Mode—Displays one of the following options:
  - Native Stacking—Device is part of a stack in which all of the units are of the same type.
  - Hybrid Stacking—Device is part of a stack that can consist of multiple switches within the same series.
- Stack Topology—Displays whether the topology of the stack is chain or ring.
- Stack Active Unit—Displays the unit ID of the active unit of the stack.

Stack Topology View

This view provides a graphical view of the device. Hovering over it displays the unit number, its function in the stack and the devices that it is connected to in the stack and through which stacking ports.

Unit View and Stack Port Configuration

When you click on a specific device in the Stack Topology View, a graphical view of the device is seen.

Step 2 To select stack ports for a device:

a. Click a device in the Stack Topology View. The ports on this device are displayed in the Unit View and Stack Port Configuration.

b. When you hover over a port, a tool tip displays the stacking port number, unit that it is connected to (if there is one), the port speed and its connection status.

Step 3 To configure unit ID after reset for devices in the stack, click the device in the Stack Topology View, and enter the following field:

- Unit ID After Reset—Select a unit ID or select Auto to have the unit ID be assigned by the system.
- Unit x Stack Connection Speed—Displays the speed of the stack connection.

Step 4 Click **Apply and Reboot**. The parameters are copied to the Running Configuration file and the stack is rebooted.

User Accounts

The User Accounts page enables entering additional users that are permitted to access to the device (read-only or read-write) or changing the passwords of existing users. A user accessing the device for the first time uses the cisco/cisco username and password. After providing the default credentials, you're prompted to replace the default level 15 username and password, and you must provide a new username and password. The new password must comply with the password complexity rules.

To add a new user, follow these steps:

Procedure

Step 1 Click **Administration** > **User Accounts**.

Step 2 In the Password Recovery Service, check **Enable** to enable password recovery.

Step 3 Click **Add** to add a new user or click **Edit** to modify a user and/or the password.

Step 4 Enter the parameters.

- User Name—Enter a new username from 0 through 20 characters. UTF-8 characters aren't permitted.
- Current Password— This will appear if editing the password for an existing user.
- Suggest Password— Click to auto generate a password.
- Password—Enter a password (UTF-8 characters aren't permitted).

Note
Please refer to the password complexity rule section in Login Settings, on page 262 before creating a password.

Note
The password entered by the user is compared to a list of well known common passwords. If the password contains words from this list, the password will be rejected and a new one will need to be entered.

- Confirm Password—Enter the password again.
- Password Strength Meter—Displays the strength of password.
- User Level—Select the privilege level of the user.
  - Read-Only CLI Access (1)—User can't access the GUI and can only access CLI commands that don't change the device configuration.
  - Read/Limited Write CLI Access (7)—User can't access the GUI and can only access some CLI commands that change the device configuration. See the *CLI Reference Guide* for more information.
  - Read/Write Management Access (15)—User can access the GUI and can configure the device.

Step 5 Click **Apply**. The user is added to the Running Configuration file of the device.

Note

The password is stored in the configuration files as a non-recoverable hash using Password Based Key Derivation Function 2 (PBKDF2) with Secure Hash Algorithm, and SHA-512 as the hashing algorithm.

Idle Session Timeout

The Idle Session Timeout configures the time intervals that the management sessions can remain idle before they timeout.

To set the idle session timeout for various types of sessions, complete these steps:

Procedure

Step 1 Click **Administration** > **Idle Session Timeout**.

Step 2 Select the timeout for each type of session from the list.

- HTTP Session Timeout
- HTTPS Session Timeout
- Console Session Timeout
- Telnet Session Timeout
- SSH Session Timeout

The default timeout value is 10 minutes. You must log in again to reestablish one of the chosen sessions.

Step 3 Click **Apply** to set the configuration settings on the device.

Time Settings



Note This setting is only available in the Advanced Mode view.

Synchronized system clocks provide a frame of reference between all devices on the network. Network time synchronization is critical because every aspect of managing, securing, planning, and debugging a network involves determining when events occur. Without synchronized clocks, accurately correlating log files between devices when tracking security breaches or network usage is impossible. Synchronized time also reduces confusion in shared file systems, as it is important for the modification times to be consistent, regardless of the machine on which the file systems reside. For these reasons, it is important that the time configured on all of the devices on the network is accurate.

Real Time Clock

Some devices have an internal self-sufficient Real Time Clock (RTC) component that keeps time even when the device is shut down and not connected to a power source. This internal clock is initialized during manufacturing and can be updated by the time features of the device when the software clock is set. When a device with a functional RTC component starts up, the system clock is set to the time and date of the RTC. The RTC component is updated whenever the system clock is changed - either dynamically by the Simple Network Time Protocol (SNTP), or manually.

Note The device supports SNTP, and when enabled, the device dynamically synchronizes the device time with time from an SNTP server. The device operates only as an SNTP client, and cannot provide time services to other devices.

System Time

Use the System Time page to select the system time source. If the source is manual, you can enter the time here.

Caution If the system time is set manually and the device is rebooted, the manual time settings must be reentered.

To define system time, complete these steps:

Procedure

Step 1 Click **Administration** > **Time Settings** > **System Time**.

The following fields are displayed:

- Actual Time— Actual system time on the device.
- Last Synchronized Server—Address, stratum and type of the SNTP server from which system time was last taken.

Step 2 Enter the following parameters:

- Clock Source Settings—Select the source used to set the system clock.
  - Main Clock Source (SNTP Servers)—If this is enabled, the system time is obtained from an SNTP server. To use this feature, you must also configure a connection to an SNTP server in the SNTP Multicast/Anycast, on page 67.
  - Alternate Clock Source (PC via active HTTP/HTTPS sessions)— Check **Enable** to enable the date and time from the configuring computer using the HTTP protocol.

    Note
    The Clock Source Setting must be set to either of the above for RIP MD5 authentication to work.

- Manual Settings—Set the date and time manually. The local time is used when there's no alternate source of time, such as an SNTP server:

- Date—Enter the system date.
- Local Time—Enter the system time.

- Time Zone Settings—The local time is used via the DHCP server or Time Zone offset.
  - Get Time Zone from DHCP—Select to enable dynamic configuration of the time zone and the DST from the DHCP server. Whether one or both of these parameters can be configured depends on the information found in the DHCP packet. If this option is enabled, DHCP client must be enabled on the device.
  - Time Zone from DHCP—Displays the acronym of the time zone configured from the DHCP server. This acronym appears in the Actual Time field.
  - Time Zone Offset—Select the difference in hours between Greenwich Mean Time (GMT) and the local time. For example, the Time Zone Offset for Paris is GMT +1, while the Time Zone Offset for New York is GMT – 5.
  - Time Zone Acronym—Enter a name that represents this time zone. This acronym appears in the Actual Time field.

- Daylight Savings Settings—Select how DST is defined:
  - Daylight Savings—Select to enable Daylight Saving Time.
  - Time Set Offset—Enter the number of minutes offset from GMT ranging 1—1440. The default is 60.
  - Daylight Savings Type—Click one of the following:

    USA—DST is set according to the dates used in the USA.

    European—DST is set according to the dates used by the European Union and other countries that use this standard.

    By dates—DST is set manually, typically for a country other than the USA or a European country. Enter the parameters described below.

    Recurring—DST occurs on the same date every year.

    Selecting By Dates allows customization of the start and stop of DST:

- From—Day and time that DST starts.
- To—Day and time that DST ends.

Step 3 Selecting Recurring allows different customization of the start and stop of DST:

- From—Date when DST begins each year.
  - Day—Day of the week on which DST begins every year.
  - Week—Week within the month from which DST begins every year.
  - Month—Month of the year in which DST begins every year.
  - Time—The time at which DST begins every year.

- To—Date when DST ends each year. For example, DST ends locally every fourth Friday in October at 5:00 a.m.. The parameters are:

- Day—Day of the week on which DST ends every year.
- Week—Week within the month from which DST ends every year.
- Month—Month of the year in which DST ends every year.
- Time—The time at which DST ends every year.

Step 4 Click **Apply**. The system time values are written to the Running Configuration file.

SNTP Unicast

SNTP synchronizes a computer's system time with a server that has already been synchronized by a source such as a satellite receiver or modem. SNTP supports unicast, multicast and anycast operating modes. In unicast mode, the client sends a request to a dedicated server by referencing its unicast address.Up to 16 Unicast SNTP servers can be configured.

Note The Main Clock Source (SNTP Servers) System Time, on page 64 must be enable for SNTP Client Unicast to operate.

To add a Unicast SNTP server, follow these steps:

Procedure

Step 1 Click **Administration** > **Time Settings** > **SNTP Unicast**.

Step 2 Configure the following fields:

SNTP Client Unicast	Select to enable the device to use SNTP-predefined Unicast clients with Unicast SNTP servers.
IPv4 Source Interface	Select the IPv4 interface used for communication with the SNTP server.
IPv6 Source Interface	Select the IPv6 interface used for communication with the SNTP server. **Note** If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

Step 3 Click **Add** to add a Unicast SNTP server.

Note
To remove all user-defined SNTP servers, click **Restore Default Servers**.

Step 4 Enter the following parameters:

Server Definition	Select the SNTP server to be identified by its IP address or by name from the list.

IP Version	Select the version of the IP address: Version 6 or Version 4.
IPv6 Address Type	Select the IPv6 address type (if IPv6 is used). The options are: • Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration. • Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
Link Local Interface	Select the link local interface (if IPv6 Address Type Link Local is selected) from the list.
SNTP Server IP Address/Name	Enter the SNTP server IP address or name. The format depends on which address type was selected.
Poll Interval	Select to enable polling of the SNTP server for system time information. All NTP servers that are registered for polling are polled, and the clock is selected from the server with the lowest stratum level that is reachable. The server with the lowest stratum is considered to be the primary server. The server with the next lowest stratum is a secondary server, and so forth. If the primary server is down, the device polls all servers with the polling setting enabled, and selects a new primary server with the lowest stratum.
Authentication	Select the check box to enable authentication.
Authentication Key ID	If authentication is enabled, select the value of the key ID.

Step 5 Click **Apply**. The STNP server is added, and you are returned to the main page.

SNTP Multicast/Anycast

Note This setting is only available in the Advanced Mode view.

Note The Main Clock Source (SNTP Servers) System Time, on page 64 must be enable for SNTP Client Unicast to operate.

To enable receiving SNTP packets from all servers on the subnet and/or to enable transmitting time requests to SNTP servers, follow these steps:

Procedure

Step 1 Click **Administration** > **Time Settings** > **SNTP Multicast/Anycast**.

Select from the following options:

Option	Description
SNTP IPv4 Multicast Client Mode (Client Broadcast Reception)	Select to receive system time IPv4 Multicast transmissions from any SNTP server on the subnet.
SNTP IPv6 Multicast Client Mode (Client Broadcast Reception)	Select to receive system time IPv6 Multicast transmissions from any SNTP server on the subnet.
SNTP IPv4 Anycast Client Mode (Client Broadcast Transmission)	Select to transmit SNTP IPv4 synchronization packets requesting system time information. The packets are transmitted to all SNTP servers on the subnet.
SNTP IPv6 Anycast Client Mode (Client Broadcast Transmission)	Select to transmit SNTP IPv6 synchronization packets requesting system time information. The packets are transmitted to all SNTP servers on the subnet.

Step 2 Click **Add** to select the interface for SNTP.

Select an interface and configure the settings.

Step 3 Click **Apply** to save the settings to the Running Configuration file.

SNTP Authentication

Note This setting is only available in the Advanced Mode view.

SNTP clients can authenticate responses by using HMAC-MD5. An SNTP server is associated with a key. This is used as input together with the response itself to the MD5 function; the result of the MD5 is also included in the response packet. The SNTP Authentication page enables configuration of the authentication keys that are used when communicating with an SNTP server.

The authentication key is created on the SNTP server in a separate process that depends on the SNTP server type. Consult with the SNTP server system administrator for more information.

Procedure

Step 1 Click **Administration** > **Time Settings** > **SNTP Authentication**.

Step 2 Select **SNTP Authentication** to support authentication of an SNTP session between the device and an SNTP server.

Step 3 Click **Apply** to update the device.

Step 4 Click **Add.**

Step 5 Enter the following parameters:

- Authentication Key ID—Enter the number used to identify this SNTP authentication key internally.
- Authentication Key (Encrypted)—Enter the key used for authentication (up to eight characters) in encrypted format. The SNTP server must send this key for the device to synchronize to it.

- Authentication Key (Plaintext)—Enter the key used for authentication (up to eight characters) in plaintext format. The SNTP server must send this key for the device to synchronize to it.
- Trusted Key—Select to enable the device to receive synchronization information only from a SNTP server by using this authentication key.

Step 6 Click **Apply**. The SNTP Authentication parameters are written to the Running Configuration file.

Time Range

Time ranges can be defined and associated with the following types of commands, so that they are applied only during that time range:

- Port Stat
- Time-Based PoE

There are two types of time ranges:

- Absolute—This type of time range begins on a specific date or immediately and ends on a specific date or extends infinitely. It is created in the Time Range pages. A periodic element can be added to it.
- Periodic—This type of time range contains a time range element that is added to an absolute range, and begins and ends on a periodic basis. It is defined in the Periodic Range pages.

If a time range includes both absolute and periodic ranges, the process associated with it is activated only if both absolute start time and the periodic time range have been reached. The process is deactivated when either of the time ranges are reached. The device supports a maximum of 20 absolute time ranges.

To ensure that the time range entries take effect at the desired times, the system time must be set.The time-range feature can be used for the following:

- Limit access of computers to the network during business hours (for example), after which the network ports are locked, and access to the rest of the network is blocked (see Configuring Ports and Configuring LAG Settings)
- Limit PoE operation to a specified period.

  Add these descriptions for time range

Procedure

Step 1 Click **Administration** > **Time Settings** > **Time Range**.

Step 2 In the Time Range Table, click **Add** to add a new time range or **Edit** or **Delete** to edit or delete an existing one.

Step 3 To add a new time range, click **Add** and configure the following:

- Time Range Name—Enter a name for your time range
- Absolute Starting Time—Select Immediate or enter a date and time.
- Absolute Ending Time—Select Infinite or enter a date and time

Step 4 Click **Apply** to apply the new time range settings.

Recurring Time Range



Note This setting is only available in the Advanced Mode view.

A recurring time element can be added to an absolute time range. This limits the operation to certain time periods within the absolute range.

To add a recurring time range element to an absolute time range:

Procedure

Step 1 Click **Administration** > **Time Settings** > **Recurring Range**.

The existing recurring time ranges are displayed (filtered per a specific, absolute time range.)

Step 2 Select the absolute time range to which to add the recurring range.

Step 3 To add a new recurring time range, click **Add**.

Step 4 Enter the following fields:

- Recurring Starting Time—Enter the day of the week, and time that the Time Range begins.
- Recurring Ending Time—Enter the day of the week, and time that the Time Range ends.

Step 5 Click **Apply.**

System Log

This section describes the system logging, which enables the device to generate multiple independent logs. Each log is a set of messages describing system events.

The device generates the following local logs:

- Log sent to the console interface.
- Log written into a cyclical list of logged events in the RAM and erased when the device reboots.
- Log written to a cyclical log-file saved to the Flash memory and persists across reboots.

In addition, you can send messages to remote SYSLOG servers in the form of SNMP traps and SYSLOG messages.

Log Settings

Note The Console Setting is only available in the Advanced Mode view)

You can select the events to be logged by severity level. Each log message has a severity level marked with the first letter of the severity level concatenated with a dash (-) on each side (except for Emergency that is indicated by the letter F). For example, the log message "%INIT-I-InitCompleted: … " has a severity level of I, meaning Informational.

The event severity levels are listed from the highest severity to the lowest severity, as follows:

- Emergency—System is not usable.
- Alert—Action is needed.
- Critical—System is in a critical condition.
- Error—System is in error condition.
- Warning—System warning has occurred.
- Notice—System is functioning properly, but a system notice has occurred.
- Informational—Device information.
- Debug—Detailed information about an event.

You can select different severity levels for RAM and Flash logs. These logs are displayed in the RAM Memory, on page 57 and Flash Memory, on page 57, respectively.

Selecting a severity level to be stored in a log causes all of the higher severity events to be automatically stored in the log. Lower severity events are not stored in the log. For example, if Warning is selected, all severity levels that are Warning and higher are stored in the log (Emergency, Alert, Critical, Error, and Warning). No events with severity level below Warning are stored (Notice, Informational, and Debug).

To set global log parameters, complete the following steps:

Procedure

Step 1 Click **Administration** > **System Log** > **Log Settings**.

Step 2 Enter the parameters.

Logging	Select to enable message logging.
Syslog Aggregator	Select to enable the aggregation of SYSLOG messages and traps. If enabled, identical and contiguous SYSLOG messages and traps are aggregated over the specified Max. Aggregation Time and sent in a single message. The aggregated messages are sent in the order of their arrival. Each message states the number of times it was aggregated.
Max. Aggregation Time	Enter the interval of time that SYSLOG messages are aggregated.

Originator Identifier	Enables adding an origin identifier to SYSLOG messages. The options are: • None—Do not include the origin identifier in SYSLOG messages. • Hostname—Include the system host name in SYSLOG messages. • IPv4 Address—Include the IPv4 address of the sending interface in SYSLOG messages. • IPv6 Address—Include the IPv6 address of the sending interface in SYSLOG messages. • User Defined—Enter a description to be included in SYSLOG messages.
RAM Memory Logging	Select the severity levels of the messages to be logged to the RAM.
Flash Memory Logging	Select the severity levels of the messages to be logged to the Flash memory.

Step 3 Click **Apply**. The Running Configuration file is updated.

Remote Logging Settings

The Remote Log Servers page enables defining remote SYSLOG servers to which log messages are sent. For each server, you can configure the severity of the messages that it receives.

To define SYSLOG servers, follow these steps:

Procedure

Step 1 Click **Administration** > **System Log** > **Remote Log Servers**.

Step 2
Note
This setting is only available in the Advanced Mode view)

Enter the following fields:

- IPv4 Source Interface—Select the source interface whose IPv4 address will be used as the source IPv4 address of SYSLOG messages sent to SYSLOG servers.
- IPv6 Source Interface—Select the source interface whose IPv6 address will be used as the source IPv6 address of SYSLOG messages sent to SYSLOG servers.

  Note
  If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

  Information is described for each previously configured log server. The fields are described below in the Add page.

Step 3 Click **Add**.

Step 4 Enter the parameters.

Server Definition	Select whether to identify the remote log server by IP address or name.
IP Version	Select the supported IP format.
IPv6 Address Type	Select the IPv6 address type (if IPv6 is used). The options are: • Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80::/10, isn't routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration. • Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
Link Local Interface	Select the link local interface (if IPv6 Address Type Link Local is selected) from the list.
Log Server IP Address/Name	Enter the IP address or domain name of the log server.
UDP Port	Enter the UDP port to which the log messages are sent.
Facility	Select a facility value from which system logs are sent to the remote server. Only one facility value can be assigned to a server. If a second facility code is assigned, the first facility value is overridden.
Description	Enter a server description.
Minimum Severity	Select the minimum level of system log messages to be sent to the server.

Step 5 Click **Apply.** The Add Remote Log Server page closes, the SYSLOG server is added, and the Running Configuration file is updated.

File Management

A File Management System is an application that is used to store, arrange and access the files that are on your device. The system files are files that contain information, such as: configuration information or firmware images. Generally, every file under the flash://system/ folder is a system file. Various actions can be performed with these files, such as: selecting the firmware file from which the device boots, modifying various types of configuration files internally on the device, or copying files to or from an external device, such as an external server.

The following are some of the types of files are found on the device:

- Running Configuration—Contains the parameters currently being used by the device to operate. This file is modified when you change parameter values on the device. If the device is rebooted, the Running Configuration is lost. To preserve any changes you made to the device, you must save the Running Configuration to the Startup Configuration, or another file type.
- Startup Configuration—The parameter values that saved by copying another configuration (usually the Running Configuration) to the Startup Configuration. The Startup Configuration is retained in Flash and

is preserved when the device is rebooted. At this time, the Startup Configuration is copied to RAM and identified as the Running Configuration.

- Mirror Configuration—A copy of the Startup Configuration, created by the device when the following conditions exist:
  - The device has been operating continuously for 24 hours.
  - No configuration changes have been made to the Running Configuration in the previous 24 hours.
  - The Startup Configuration is identical to the Running Configuration.

  Only the system can copy the Startup Configuration to the Mirror Configuration. However, you can copy from the Mirror Configuration to other file types or to another device.
- Backup Files—Manual copies of a files used for protection against system shutdown or for the maintenance of a specific operating state. For instance, you can copy the Mirror Configuration, Startup Configuration, or Running Configuration to a Backup file. The Backup exists in Flash or on a PC or USB drive and is preserved if the device is rebooted.
- Firmware—The program that controls the operations and functionality of the device. More commonly referred to as the image.
- Language File—The dictionary that enables the web-based configuration utility windows to be displayed in the selected language.
- Logging File—SYSLOG messages stored in Flash memory.

Firmware Operations

The Firmware Operations page can be used to:

- Update or backup the firmware image
- Swap the active image.

The software images of the units in a stack must be identical to ensure proper stack operations. Stack units can be upgraded in any one of the following ways.

Procedure

Step 1 Click **Administration** > **File Management** > **Firmware Operations**.

The following fields are displayed:

- Active Firmware File—Displays the current, active firmware file.
- Active Firmware Version—Displays the version of the current, active firmware file.

Step 2 Select the Operation Type from the following options:

- Update Firmware
- Backup Firmware

- Swap Image

Step 3 Select the Copy Method from the following options:

HTTP/HTTPS	For HTTP/HTTPS, enter the file name in the File Name field, or browse to locate and select the file.
USB	For USB, enter the file name in the File Name field, or browse to locate and select the file.
TFTP	For TFTP, proceed with the TFTP Instructions below.
SCP (File transfer via SSH)	For SCP, proceed with the SCP Instructions below.

TFTP Instructions

Note
This setting is only available in the Advanced Mode view.

Configure the following if you selected the TFTP as your copy method for the firmware operations.

Server Definition	Select from the following options: • By IP Address • By Name
IP Version	Select from the following options: • IP Version 6 • IP Version 4
IPv6 Address Type	Select from the following options: • Link Local—A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network. • Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
Link Local Interface	If for the IPv6 address type, you selected Link Local, select the interface from the drop down list.
Server IP Address/Name	Enter the server IP address/name.
Source	Enter the name of the source (0- 160 characters used)

SCP Instructions

Note
This setting is only available in the Advanced Mode view.

Configure the following if you selected the SCP as your copy method for the firmware operations.

Remote SSH Server Authentication	To enable SSH server authentication (which is disabled by default), click **Edit** .
SSH Client Authentication	Select from the following: • Use SSH Client System Credentials. • Use SSH Client One-Time Credentials:
Username	Enter the username if using the SSH Client One-Time Credentials option.
Password	Enter the password if using the SSH Client One-Time Credentials option.
Server Definition	Select from the following options: • By IP Address • By Name
IP Version	Select from the following options: • Version 6 • Version 4
IPv6 Address Type	Select from the following options: • Link Local—A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network. • Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
Link Local Interface	If for the IPv6 address type, you selected Link Local, select the interface from the drop down list.
Server IP Address/Name	Enter the server IP address/name.
Source	Enter the name of the source (0- 160 characters used)

Step 4 Click **Apply** to save your settings.

File Operations

Procedure

Step 1 Click **Administration** > **File Management** > **File Operations**.

Step 2 Select the Operation Type from the following options:

- Update File

- Backup File
- Duplicate

Step 3 Select the Destination File Type from the following options:

- Running Configuration
- Startup Configuration
- Mirror Configuration
- Logging File
- Language File
- Dashboard Info File

Step 4 Select the Copy Method from the following options:

HTTP/HTTPS	For HTTP/HTTPS, enter the file name in the File Name field, or browse to locate and select the file.
USB	For USB, enter the file name in the File Name field, or browse to locate and select the file.
Internal Flash	For Internal File, enter the file name in the File name field or click on File Directory to browse and to locate. Sensitive Data Handling -Select the method in which the data should be handled. This applies only for file backup or duplication. • Exclude - to exclude sensitive data • Encrypt - to encrypt sensitive data • Plaintext - to display sensitive data in plaintext.
TFTP	For TFTP, proceed with the TFTP Instructions below.
SCP (File transfer via SSH)	For SCP, proceed with the SCP Instructions below.

TFTP Instructions

Configure the following if you selected the TFTP as your update or backup method for the file operations.

Server Definition	Select from the following options: • By IP Address • By Name
IP Version	Select from the following options: • IP Version 6 • IP Version 4

IPv6 Address Type	Select from the following options: • Link Local—A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network. • Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
Link Local Interface	If for the IPv6 address type, you selected Link Local, select the interface from the drop down list.
Server IP Address/Name	Enter the server IP address/name.
Source	Enter the name of the source (0 - 160 characters used)

SCP Instructions

Configure the following if you selected the SCP as your copy method for the file operations.

Remote SSH Server Authentication	To enable SSH server authentication (which is disabled by default), click **Edit** .
SSH Client Authentication	Select from the following: • Use SSH Client System Credentials: • Use SSH Client One-Time Credentials:
Username	Enter the username if using the SSH Client One-Time Credentials option.
Password	Enter the password if using the SSH Client One-Time Credentials option.
Server Definition	Select from the following options: • By IP Address • By Name
IP Version	Select from the following options: • IP Version 6 • IP Version 4
IPv6 Address Type	Select from the following options: • Link Local—A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network. • Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
Link Local Interface	If for the IPv6 address type, you selected Link Local, select the interface from the drop down list.
Server IP Address/Name	Enter the server IP address/name.

Source	Enter the name of the source (0 - 160 characters used)

Step 5 In the File name section, click the **Browse** button to locate and select the file.

Step 6 Click **Apply**.

File Directory

The File Directory page displays the system files existing in the system.

Procedure

Step 1 Click **Administration** > **File Management** > **File Directory**.

Step 2 If required, enable Auto Mirror Configuration. This enables the automatic creation of mirror configuration files. When disabling this feature, the mirror configuration file, if it exists, is deleted.

Step 3 Select the drive from which you want to display the files and directories. The following options are available:

- Flash—Display all files in the root directory of the management station.
- USB—Display files on the USB drive.

Step 4 Click **Go** to display the following fields:

- File Name—Type of system file or actual name of file depending on the file type.
- Permissions—Read/write permissions of the user for the file.
- Size—Size of file.
- Last Modified—Date and time that file was modified.
- Full Path—Path of file.

DHCP Auto Update

The Auto Configuration/Image Update feature provides a convenient method to automatically configure switches in a network and upgrade their firmware. This process enables the administrator to remotely ensure that the configuration and firmware of these devices in the network are up to date.

Procedure

Step 1 Click **Administration** > **File Management** > **DHCP Auto Update**.

Step 2 Configure the following:

Auto Configuration Via DHCP	Check to enable the auto configuration via DHCP. The Auto Configuration feature provides a convenient method to automatically configure switches in a network and upgrade their firmware.
Download Protocol	Select the download protocol from the following options: • Auto By File Extension—(Default) Files with this extension are downloaded using SCP (over SSH), while files with other extensions are downloaded using TFTP. • TFTP Only—The download is done through TFTP, regardless of the file extension of the configuration file name. • SCP Only—The download is done through SCP (over SSH), regardless of the file extension of the configuration file name.
Image Auto Update via DHCP:	Check to enable image auto update via DHCP. The Image Auto Update feature provides a convenient method to automatically update switches in a network and upgrade their firmware.
Download Protocol	Select the download protocol from the following options: • Auto By File Extension—(Default) Files with this extension are downloaded using SCP (over SSH), while files with other extensions are downloaded using TFTP. • TFTP Only—The download is done through TFTP, regardless of the file extension of the configuration file name. • SCP Only—The download is done through SCP (over SSH), regardless of the file extension of the configuration file name.

Step 3 Select the SSH settings for SCP.

Remote SSH Server Authentication:	Click the link to navigate to the SSH Server Authentication page. There you can enable authentication of the SSH server to be used for the download and enter the trusted SSH server if required.
SSH Client Authentication	• Click on the **System Credentials** to enter user credentials in the SSH User Authentication page.
Backup Server Definition	Select from the following options: • By IP Address • By Name
IP Version	Select from the following options: • IP Version 6 • IP Version 4

IPv6 Address Type	Select from the following options: • Link Local—A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network. • Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
Link Local Interface	If for the IPv6 address type, you selected Link Local, select the interface from the drop down list.
Backup Server IP Address/Name	Enter the name of the backup configuration file.
Backup Configuration File Name	Enter the name of the backup configuration file (0- 160 characters used)
Backup Indirect Image File Name	Enter the name of backup indirect image file (0- 160 characters used).
Last Auto Configuration / Image Server IP Address	The address of the last auto configuration/image server IP address is displayed.
Last Auto Configuration File Name	The name of the last auto configuration file is displayed.

Note
DHCP Auto Configuration / Image is operational only when the IP Address configuration is dynamic.

Step 4 Click **Apply** to save your settings.

Cisco Business Dashboard Settings

Cisco Business Dashboard helps you monitor and manage your Cisco 100 to 500 Series network with the use of the Cisco Business Dashboard Manager. The Cisco Business Dashboard Manager is an add-on that automatically discovers your network and allows you to configure and monitor all supported Cisco 100 to 500 Series devices such as Cisco switches, routers, and wireless access points.

You can view the Cisco Business Dashboard by clicking Request a Demo

Cisco Business Dashboard Manager is a distributed application which is comprised of two separate components or applications: one or more Probes referred to as Cisco Business Dashboard Probe and a single Manager called Cisco Business Dashboard Manager. An instance of Cisco Business Dashboard Probe is installed at each site in the network, performs network discovery and communicates directly with each Cisco device.

Note For detailed instructions on how to setup the Cisco Business Dashboard Manager and Probe, please consult the Cisco Business Dashboard Quick Start Guide.

https://cisco.com/go/cbd-docs

Complete the following steps on the switch graphical user interface (GUI) to enable a Probe connection to a Dashboard, configure the Organization and Network name, and other information required to allow connection to the Dashboard:

Procedure

Step 1 Click **Administration** > **Cisco Business Dashboard Settings**.

Step 2 Configure the following:

Probe Operation	Check to enable the Cisco Business Dashboard Probe operation.
Probe Status	Displays the status of the CBD probe. Possible value are Active, Inactive or Fault. If the probe status is Active then alongside the probe status "Active" the probe mode will also be displayed as follows: • Active (Probe Managed) - The Probe performs network discovery and communicates directly with each managed device on behalf of the Dashboard. In one network you should only enable one Probe. • Active (Direct Managed) - Direct managed devices will discover other devices in the broader network and connect those devices to the Dashboard automatically then those devices become manageable. You may optionally have the dashboard explicitly search the IP address ranges to discover network devices, which can be in other VLANs or subnets. Direct managed network is recommended if all your devices support direct management.
Probe Version	Displays the version of the Cisco Business Dashboard probe.
Logging Threshold	Select one of the following options (Information, Debug, Warning, or Error) from the drop-down list to limit the level of messages logged by the Cisco Business Dashboard probe agent. Only messages with the specified level or higher will be logged.
All Module Logging	Check to enable. This logs all communication and events between all modules.
Call Home Logging	Check to enable. This logs all communication between the Probe and Manger.
Discovery Logging	Check to enable. This logs the device discovery events and topology discovery.
Services Logging	Check to enable. This logs the message translation between northbound and southbound.
System Logging	Check to enable. This logs the core system process not covered by any of the other logs.
Northbound Logging	Check to enable. This logs the communication between the Manager and the Probe.
Southbound Logging	Check to enable. This logs the low level communication between the Probe and devices.
Dashboard Connection	Check to enable connection.

Dashboard Status	Displays the status (Connected or Disconnected) of the Cisco Business Dashboard Manager. If the Dashboard Status is "Disconnected" an error reason will be displayed. Here are some examples: • Certificate-error- unspecified certificate verification error • Certificate-error- certificate is not yet valid • Certificate-error- certificate has expired • Certificate-error- certificate verify failed • Connection-error- Host not found (authoritative) • Connection-error- No route to host
Dashboard Definition	Define the address of the Cisco Business Dashboard. Select one of the following: • By IP address- this option requires you to enter a valid IP address to the IP Address/Name field. • By Name- this option requires you to enter a host name to the IP Address/Name field.
IP Address/Name	Enter the name or IP address of the Cisco Business Dashboard.
Dashboard Port	Specify one of the following TCP ports to connect to the Dashboard. • Use Default (443). • User Defined (Range: 1-65535). This option is available only if a valid address is entered in the Dashboard Address field.
Connection Setup	Specify one of the following connection setups: • Online with Web Browser • Offline with Access Key
Access Key ID	The Access Key ID field consists of 24 hexadecimal digits. Note that the field should only allow the input of hexadecimal characters.
Access Key Secret	Specify the secret to use for authentication. It can be Encrypted or in Plaintext format. The Plaintext format is specified as an alphanumeric string without white-spaces (up to 160 chars). The Key ID and Secret settings must be set together. **Note** When applying, if the Key ID field is empty and the Secret field is not, or if the Secret field is empty and the Key ID field is not, the following error message is displayed: “Key ID and Secret must be set together”.

Step 3 Click **Apply** to save the setting to the running configuration.

Note

The fields Organization Name, Network Name, Dashboard Address, Key ID cannot be modified if Dashboard Connection setting is enabled. To modify any of these settings clear the Dashboard Connection check box, click **Apply**, and redo steps 2-4 above.

Display Sensitive Data as Plaintext- Click to display the sensitive data a plain text.

Reset Connection - click to disconnect the current connection with the Dashboard, flush the Cisco Business Dashboard Probe cached data, and then attempt to reconnect to the Dashboard. A confirmation message is displayed before the operation starts. This control is enabled only if the Dashboard Connection and Probe Operation are enabled.

Note
The Reset Connection is only enabled if the Dashboard Connection and Probe Operation check boxes are checked.

Clear Probe Database- Click to clear the probe data. It is enabled only if the Probe Operation checkbox is unchecked (and has been unchecked since the screen loaded). Otherwise, the button is disabled with the following tooltip: “Probe Operation must be disabled prior to clearing probe database”.

Note
Many factors affect the number of network devices and clients that the Cisco Business Dashboard Probe on a switch can manage. We recommend that a probe on a switch manage no more than 15 network devices (switches, routers, and wireless access points) and no more than 150 connected clients. If your network is more complex, we recommend that you use other platforms for the Cisco Business Dashboard Probe. For more information about Cisco Business Dashboard, go to https://www.cisco.com/c/en/us/products/cloud-systems-management/business-dashboard/index.html.

Plug-n-Play (PNP)

Installation of new networking devices or replacement of devices can be expensive, time-consuming and error-prone when performed manually. Typically, new devices are first sent to a central staging facility where the devices are unboxed, connected to a staging network, updated with the right licenses, configurations and images; then packaged and shipped to the actual installation location. After these processes are completed, experts must travel to the installation locations to perform the installation. Even in scenarios where the devices are installed in the NOC/Data Center itself, there may not be enough experts for the sheer number of devices. All these issues contribute to delays in deployment and add to the operational costs.

Connecting to PNP Server

To allow the switch to connect to the PnP server, a discovery process takes place, in which the switch discovers the PNP server address/url. There are multiple discovery methods, and they are executed by the switch according to the sequence detailed below. If a PnP server is discovered by a certain method, the discovery process is completed and the rest of the methods are not executed:

1. User configured address- the PnP server URL or IP address are specified by the user.
2. Address received from DHCP response option 43- the PnP server URL or IP address are received as part of option 43 in the DHCP response
3. DNS resolution of host name "pnpserver"- the PnP server IP addressed is obtained via DNS server resolution of host name “pnpserver”.
4. Cisco Plug and Play Connect - a redirection service that allows full “out of the box” PNP server discovery which runs over HTTPs.

The switch contacts the redirection service using the FQDN “devicehelper.cisco.com”.

Cisco PnP Connect Prerequisites

To allow Cisco Plug and Play Connect operation, the user needs to create devices and controller profiles in Plug and Play Connect (navigate to https://software.cisco.com and click the PnP Connect link). Note that a Cisco Smart Account is required to use PnP Connect. To create or update a Smart Account, see the Administration section of https://software.cisco.com.

In addition, the following prerequisites are required to be met on the switch itself:

- The PNP server was not discovered by the other discovery methods
- The device is able to successfully resolve the name devicehelper.cisco.com (either static configuration or using DNS server)
- System time was set using one of the following methods
  - Time was updated by an SNTP server
  - Clock was set manually by user
  - Time was preserved across resets by Real Time Clock (RTC).

CA-Signed Certificate based Authentication

Cisco distributes certificates signed by a signing authorities in .tar file format and signs the bundle with Cisco Certificate Authority (CA) signature. This certificate bundle is provided by Cisco infoSec for public downloads on cisco.com.

Note If the PNP server discovery is based on Cisco PnP Connect, the trust-pool is downloaded from following: http://www.cisco.com/security/pki/trs/ios_core.p7b.

If the PNP server discovery is based on DHCP option 43, use the “T<Trust pool CA bundle URL>;” parameter in DHCP option 43 to provide the URL for downloading the trust pool. The certificates from this bundle can be installed on the Cisco device for server-side validation during SSL handshake. It is assumed that the server uses a certificate, which is signed by one of the CA that is available in the bundle.

The PnP agent uses the built-in PKI capability to validate the certificate bundle. As the bundle is signed by Cisco CA, the agent is capable of identifying a bundle that is tampered before installing the certificates on the device. After the integrity of the bundle is ensured by the agent, the agent installs the certificates on the device. After the certificates are installed on the device, the PnP agent initiates an HTTPs connection to the server without any additional steps from the server.

Note The device also supports a built in certificate bundle which is installed as part of the bootup process. this bundle can be used to validate PNP server. If a Bundle is downloaded based on Cisco PnP Connect information then the certificates from the downloaded bundle are installed and the certificates based on the built in bundle are un-installed.

Note In addition to validating PNP certificate based on installed CA certificate the PNP Agent also validates that the certificate's Common Name/Subject Alternate Name (CN/SAN) matches the host name/IP address of the PNP server. If they don't match validation of certificate is rejected.

Cisco PnP DHCP Option 43 Usage Guidelines

DHCP option 43 is a vendor specific identifier which is one of the methods that can be used by the PnP agent to locate and connect to the PnP server (see Cisco Plug-n-Play for more information).

The following provides Information on configuration of Option 43 to allow proper configuration on DHCP server.

Option 43 includes the following fields/parameters:

<DHCP-typecode><feature-opcode><version><debug-option>;<arglist>

The <arglist> parameter should use the following syntax:

B<IP address type>;I<IP address>;J<Port>;K<Transport protocol>;T<Trust pool CA bundle URL>;Z<SNTP server IP address>

The following table details the description and usage of option 43 fields

Parameter	Description
DHCP-typecode	DHCP sub-option type. The DHCP sub-option type for PnP is 5.
Feature-opcode	Feature operation code – can be either Active (A) or Passive (P). The feature operation code for PnP is Active (A) which implies that PnP agent initiates a connection to the PnP server. If the PnP server cannot be reached, PnP agent retries until it makes a connection.
Version	Version of template to be used by PnP agent. Must be 1.
Debug-option	Turns ON or OFF the debug messages during the processing of the DHCP Option 43: D – debug option is ON; N – debug option is OFF.
K	Transport protocol to be used between PnP agent and PnP server: 4 - HTTP or 5 – HTTPS.
B	IP address type of PnP server IP address specified with the letter code 'I': 1- host, 2- IPv4, 3- IPv6
I	IP address or host name of PnP server. If host name is specified, DNS related options must be present in the DHCP server to allow for successful use of host name.

Parameter	Description
T	URL of trust pool CA bundle. You can get the CA bundle from a Cisco Business Dashboard, or from a TFTP server. • When using Cisco Business Dashboard, use the following URL format: http://*CBD IP address or domain name/ca/trustpool/CA_bundle_name* • When using TFTP Server, use the following URL format: tftp://*tftp server IP/CA_bundle_name*
Z	SNTP server IP address. You must sync the clock before configuring a trust pool. **Note** The switch clock is considered synchronized if it was updated by any SNTP server supported by the switch (by default, user configured or in Z parameter) or set manually by the user. This parameter is required when using trust pool security if the switch can not reach any other SNTP server. For example, for an out-of-the box switch with factory default configuration but no Internet connectivity to reach the default SNTP servers.
J	Port number HTTP=80 HTTPS=443

Examples for Option 43 usage:

- The following format is used for PnP connection setup using HTTP:

```
option 43 ascii 5A1N;K4;B2;I10.10.10.3;J80
```

- The following format is used for PnP connection setup on top of HTTPS, directly using a trust pool. HTTPS can be used when the trust pool CA bundle is downloaded from a Cisco Business Dashboard and the Cisco Business Dashboard server certificate was issued by a 3rd party (not self signed). In the example below “10.10.10.3” is the Cisco Business Dashboard IP address. Optionally, you can specify a domain name:

```
option 43 ascii
5A1N;K5;B2;I10.10.10.3;Thttp://10.10.10.3/ca/trustpool/ios.p7b;Z10.75.166.1
```

PNP Settings

To configure PNP settings, follow these steps:

Procedure

Step 1 Click **Administration** > **PNP** > **PNP Settings**.

Step 2 Configure PNP by entering information in the following fields:

PNP State	Check to enable.
PNP Transport / Settings Definition	Select one of the following options for locating configuration information, regarding the transport protocol to use, the PNP server address and the TCP port to use: • Default Settings—If this option is selected, the PNP settings are then taken from DHCP option 43. If settings aren't received from DHCP option 43, the following default values are used: default transport protocol HTTP, DNS name "pnpserver" for PNP server and the port related to HTTP. If the "pnpserver" name is not resolved by DNS, then Cisco Plug and Play Connect service is used, using DNS name "devicehelper.cisco.com". When selecting the Default Settings option, all fields in PNP Transport section are grayed out. If both PNP agent and DHCP Auto Configuration/Image Update are enabled on device- in case he DHCP reply includes, in addition to option 43, options related to config or image file name, then device ignores received option 43. • Manual Settings—Manually set the TCP port and server settings to use for PNP transport.
Transport Protocol	Select the transport protocol, HTTP or HTTPS.
TCP Port	Number of the TCP port. This is entered automatically by the system: 80 for HTTP.
Server Definition	Select whether to specify the PNP server By IP address or By name.
IP Version	Select the supported IP format. • Version 6—IPv6 • Version 4—IPv4
Server IPv6 Address Type	Select one of the following options, if the IP version type is IPv6: • Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration. • Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
Link Local Interface	If the source IPv6 address type is Link Local, select from where it is received.
Server IP Address/Name	Enter the IP address or domain name of the PNP server.
PNP User / User Definition	User information to be sent in PNP packets sent to the server. Select one of the following options: • Default Settings—When selecting this option, the PNP username and password settings are taken from DHCP option 43. If this option is selected the username and password fields are grayed out. • Manual Settings—Select to manually configure PNP username and password.

User Name	Username to be entered in the PNP packets.
Password	Password in either Encrypted or Plaintext form.
PNP Behavior Settings/Reconnection Interval	If you select User Defined, set the interval (in seconds) before attempting to reconnect the session after the connection is lost.
Discovery Timeout	Specifies the time to wait, in seconds, before attempting discovery again after a discovery of the PNP server failed.
Timeout Exponential Factor	Value that triggers the discovery attempt exponentially. By multiplying the previous timeout value by an exponential value and applying the result as timeout (if value is smaller than max timeout value).
Max Discovery Timeout	Maximum value of timeout. Must be greater than the Discovery Timeout value.
Watchdog Timeout	Interval of time to wait for a reply from a PnP or file server during an active PNP session (for example during a file download process).

Step 3 Click **Apply**. The parameters are copied to the Running Configuration file.

Click **Display Sensitive Data as Plaintext** to display the password if it's encrypted.

PNP Session

The PNP Session screen displays the value of the PNP parameters currently in effect. The source of the parameter is displayed in parenthesis where relevant.

To display information about PNP parameters, follow these steps:

Procedure

Click **Administration > PNP > PNP Session**.

The following fields are displayed:

- Administrative Status—Whether PNP is enabled or not.
- Operational Status—Is PNP operational.
- PNP Agent State—Indicates whether there's an active PNP session. The possible values are Discovery Wait; Discovery; Not Ready; Disabled; Session; Session Wait.
- Transport Protocol– Displays the PNP agent session information.
- TCP Port—TCP port of the PNP session
- Server IP Address—IP address of PNP server
- Username—Username to be sent in PNP packets.

- Password MD5—Password to be sent in PNP packets.
- Session Interval Timeout—Session Interval timeout configured (appears only when PNP Agent State is waiting).
- Remaining Timeout—Value of remaining timeout.



Note Click the Resume button to immediately take the PnP agent out of the waiting state, in the following way:

- If the agent is in the Discovery Waiting state, it's set to the Discovery state.
- If the agent is in the PnP Session Waiting state, it's set to the PnP Session state.

Reboot

Some configuration changes, such as enabling jumbo frame support, require the system to be rebooted before they take effect. However, rebooting the device deletes the Running Configuration, so it's critical to save the Running Configuration as the Startup Configuration before rebooting. Clicking Apply doesn't save the configuration to the Startup Configuration. section.

To reboot the device, follow these steps:

Procedure

Step 1 Click **Administration** > **Reboot**.

Step 2 Click **Reboot** to reboot the device.

- Reboot—Reboots the device. Since any unsaved information in the Running Configuration is discarded at reboot, you must click **Save** to preserve the current configuration across the boot process. If the Save option isn't displayed, the Running Configuration matches the Startup Configuration and no action is necessary.

  The following options are available:

  - Immediate—Reboot immediately.
  - Date—Enter the date (month/day) and time (hour and minutes) of the schedule reboot. This schedules a reload of the software to take place at the specified time (using a 24-hour clock).

    Note
    This option can only be used if the system time has either been set manually or by SNTP.

  - Click **Cancel Reboot** to cancel a scheduled reboot.
  - In—Reboot within the specified number of days, hours and minutes The maximum amount of time that can pass is 24 days.

- Restore to Factory Defaults—Reboots the device by using the factory default configuration. This process erases all except the Active Image, Inactive Image, Mirror configuration and Localization files.

- Clear Startup Configuration File—Check to clear the startup configuration on the device for the next time it boots up.

Hardware Resources

The Hardware Resources page enables you to adjust the Router TCAM allocation for policy-based routing (IPv4 and IPv6) and VLAN-mapping rules. It also enables you to view the status and to reactivate hardware-based routing.

If you change the router TCAM allocation incorrectly, an error message is displayed. If your router TCAM allocation is feasible, a message is displayed that an automatic reboot will be performed with the new settings.

Routing resources can be modified incorrectly, in one of the following ways:

- The number of router TCAM entries for a specific entry type that you allocate is less than the number currently in use.
- The total number of router TCAM entries that you allocated is greater than the maximum available.

To view and modify routing resources, follow these steps:

Procedure

Step 1 Click **Administration** > **Hardware Resources**.

The following fields are displayed:

- Maximum IPv4 Policy-Based Routes
  - Use Default—Use default values.
  - User Defined—Enter a value.
- Maximum IPv6 Policy-Based Routes
  - Use Default—Use default values.
  - User Defined—Enter a value.
- Maximum VLAN-Mapping Entries—Select one of the following options:
  - Use Default—Use default values.
  - User Defined—Enter a value.
- Hardware-Based Routing: Displays whether hardware-based routing is enabled or suspended.

Step 2 Save the new settings by clicking **Apply**.

Note If hardware-based routing isn't active, the Reactivate Hardware Based Routing button appears. Click on this button to enable hardware-based routing. Activation of hardware-based routing depends on the hardware resources that are available to support the current routing configuration. If router resources aren't sufficient to support device configuration, the operation fails and an error message is displayed to the user.

Discovery Bonjour

As a Bonjour client, the device broadcasts Bonjour Discovery protocol packets to directly connected IP subnets. The device can be discovered by a network management system or other third-party applications. By default, Bonjour is enabled on the Management VLAN.

To configure Bonjour, follow these steps:

Procedure

Step 1 Click **Administration** > **Discovery - Bonjour**.

Step 2 Select **Enable** to enable Bonjour Discovery globally.

Step 3 To enable Bonjour on a specific interface, click **Add.**

Step 4 Select and configure the interface.

Step 5 Click **Apply** to update the Running Configuration file.

Note
When Bonjour is enabled, it sends Bonjour Discovery packets to interfaces with IP addresses associated with Bonjour on the Bonjour Discovery Interface Control table.

Step 6 Click **Delete** to disable Bonjour on an interface.

Note If Bonjour is disabled, the device stops sending Bonjour Discovery advertisements and stops listening for Bonjour Discovery advertisements sent by other devices.

Discovery - LLDP

LLDP is a protocol that enables network managers to troubleshoot and enhance network management in multi-vendor environments. LLDP standardizes methods for network devices to advertise themselves to other systems, and to store discovered information. LLDP enables a device to advertise its identification, configuration, and capabilities to neighboring devices that then store the data in a Management Information Base (MIB).

LDP is a link layer protocol. By default, the device terminates and processes all incoming LLDP packets as required by the protocol. This section describes how to configure LLDP and covers the following topics:

Properties

The Properties page enables entering LLDP general parameters, such as enabling/disabling the feature globally and setting timers. To enter LLDP properties, proceed as follows:

Procedure

Step 1 Click **Administration** > **Discovery - LLDP** > **Properties**.

Step 2 Enter the parameters.

LLDP Status	Select to enable LLDP on the device (enabled by default).
LLDP Frames Handling	If LLDP isn't enabled, select one of the following options: • Filtering—Delete the packet. • Flooding—Forward the packet to all VLAN members
TLV Advertise Interval	Enter the rate in seconds at which LLDP advertisement updates are sent, or use the default.
Topology Change SNMP Notification Interval	Enter the minimum time interval between SNMP notifications.
Hold Multiplier	Enter the amount of time that LLDP packets are held before the packets are discarded, measured in multiples of the TLV Advertise Interval. For example, if the TLV Advertise Interval is 30 seconds, and the Hold Multiplier is 4, then the LLDP packets are discarded after 120 seconds.
Reinitializing Delay	Enter the time interval in seconds that passes between disabling and reinitializing LLDP, following an LLDP enable/disable cycle.
Transmit Delay	Enter the amount of time in seconds that passes between successive LLDP frame transmissions, due to changes in the LLDP local systems MIB.
Chassis ID Advertisement	Select one of the following options for advertisement in the LLDP messages: • MAC Address—Advertise the MAC address of the device. • Host Name—Advertise the host name of the device.

Step 3 In the LED-MED Properties Fast Start Repeat Count field, enter the number of times LLDP packets are sent when the LLDP-MED Fast Start mechanism is initialized. This occurs when a new endpoint device links to the device. For a description of LLDP MED, refer to the LLDP MED Network Policy section.

Step 4 Click **Apply**. The LLDP properties are added to the Running Configuration file.

Port Settings

Note This setting is only available in the Advanced Mode view.)

The LLDP Port Settings page enables LLDP and SNMP notification per port. The LLDP-MED TLVs can be configured in the LLDP MED Port Settings, on page 97.

To define the LLDP port settings, follow these steps:

Procedure

Step 1 Click **Administration** > **Discovery - LLDP** > **Port Settings**.

This page contains the port LLDP information.

Step 2 Select a port and click **Edit.**

Step 3 Configure the following fields:

Interface	Select the port to edit.
Administrative Status	Select the LLDP publishing option for the port. • Tx Only—Publishes but doesn't discover. • Rx Only—Discovers but doesn't publish. • Tx & Rx—Publishes and discovers. • Disable—Indicates that LLDP is disabled on the port.
SNMP Notification	Select **Enable** to send notifications to SNMP notification recipients.

Available/Selected Optional TLVs	Select the options to be published by the device: • Port Description—Information about the port. • System Name—System's assigned name. • System Description—Description of the network entity. • System Capabilities—Primary functions of the device, and whether these functions are enabled on the device. • 802.3 MAC-PHY—Duplex and bit rate capability and the current duplex and bit rate settings of the sending device. • 802.3 power via MDI—Maximum power transmitted via MDI • 802.3 Link Aggregation—Whether the link (associated with the port on which the LLDP PDU is transmitted) can be aggregated. • 802.3 Maximum Frame Size—Maximum frame size capability of the MAC/PHY implementation • 4-Wire Power via MDI—(relevant to PoE ports supporting 60W PoE) Proprietary Cisco TLV defined to support power over Ethernet that allows for 60 watts power (standard support is up to 30 watts). Management Address Optional TLV
Advertisement Mode	Select one of the following ways to advertise the IP management address of the device: • Auto Advertise—Specifies that the software automatically chooses a management address to advertise from all the IP addresses of the device. In case of multiple IP addresses, the software chooses the lowest IP address among the dynamic IP addresses. If there are no dynamic addresses, the software chooses the lowest IP address among the static IP addresses. • None—Select this option if no advertisement mode is desired. • Manual Advertise—Select this option and the management IP address to be advertised.
IP Address	If Manual Advertise was selected, select the Management IP address from the addresses provided.
PVID	Select to advertise the PVID in the TLV.
Port & Protocol VLAN ID	Set VLAN ID to advertise based on the port VLAN protocol.
VLAN ID	Select which VLANs will be advertised.
Protocol IDs	Select which protocols will be advertised.
Selected Protocol IDs	Select the protocols to be used in the Protocols IDs box and move them to the Selected Protocols ID box.

Step 4 Enter the relevant information, and click **Apply**. The port settings are written to the Running Configuration file.

LLDP MED Network Policy

The LLDP-MED network policy is a related set of configuration settings for a specific real-time application such as voice, or video. A network policy, if configured, can be included in the outgoing LLDP packets to the attached LLDP media endpoint device. The media endpoint device must send its traffic as specified in the network policy it receives. For example, a policy can be created for VoIP traffic that instructs VoIP phone to:

- Send voice traffic on VLAN 10 as tagged packet and with 802.1p priority 5.
- Send voice traffic with DSCP 46.

Network policies are associated with ports by using the LLDP MED Port Settings, on page 97. An administrator can manually configure one or more network policies and the interfaces where the policies are to be sent. It is the administrator's responsibility to manually create the VLANs and their port memberships according to the network policies and their associated interfaces.

In addition, an administrator can instruct the device to automatically generate and advertise a network policy for voice application based on the voice VLAN maintained by the device. Refer the Auto Voice VLAN section for details on how the device maintains its voice VLAN.

To define an LLDP MED network policy, follow these steps:

Procedure

Step 1 Click **Administration** > **Discovery - LLDP** > **LLDP MED Network Policy.**

This page contains previously-created network policies.

Step 2 Select **Auto** for LLDP-MED Network Policy for Voice Application if the device is to automatically generate and advertise a network policy for voice application based on the voice VLAN maintained by the device.

Note
When this box is checked, you may not manually configure a voice network policy.

Step 3 Click **Apply** to add this setting to the Running Configuration file.

Step 4 To define a new policy, click **Add**.

Step 5 Enter the values:

- Network Policy Number—Select the number of the policy to be created.
- Application—Select the type of application (type of traffic) for which the network policy is being defined.
- VLAN ID—Enter the VLAN ID to which the traffic must be sent.
- VLAN Type—Select whether the traffic is Tagged or Untagged.
- User Priority—Select the traffic priority applied to traffic defined by this network policy. This is the CoS value.
- DSCP Value—Select the DSCP value to associate with application data sent by neighbors. This value informs them how they must mark the application traffic they send to the device.

Step 6 Click **Apply**. The network policy is defined.

Note
You must manually configure the interfaces to include the desired manually-defined network policies for the outgoing LLDP packets using the LLDP MED Port Settings.

LLDP MED Port Settings

Note This setting is only available in the Advanced Mode view.)

The LLDP MED Port Settings page enables configuration of the LLDP-MED TLVs. Network policies are configured using the LLDP MED Network Policy page.

Note If LLDP-MED Network Policy for Voice Application is Auto and Auto Voice VLAN is in operation, then the device automatically generates an LLDP-MED Network Policy for Voice Application for all the LLDP ports. LLDP-MED enabled and are members of the voice VLAN.

To configure LLDP MED on each port, proceed as follows:

Procedure

Step 1 Click **Administration** > **Discovery - LLDP** > **LLDP MED Port Settings**.

This page displays the following LLDP MED settings for all ports:

- User-Defined Network Policy—Policies are defined for types of traffic in LLDP MED Network Policy, on page 96. The following information is displayed for the policy on the port:
  - Active—Is the type of traffic active on the port.
  - Application—Type of traffic for which the policy is defined.
- Location—Whether Location TLV is transmitted.
- PoE—Whether PoE-PSE TLV is transmitted.
- Inventory—Whether Inventory TLV is transmitted.

Step 2 The message at the top of the page indicates whether the generation of the LLDP MED Network Policy for the voice application is automatic or not. Click on the link to change the mode.

Step 3 To associate additional LLDP MED TLV and/or one or more user-defined LLDP MED Network Policies to a port, select it, and click **Edit.**

Step 4 Enter the parameters:

- Interface—Select the interface to configure.

- LLDP MED Status—Enable/disable LLDP MED on this port.
- SNMP Notification—Select whether SNMP notification is sent on a per-port basis when an end station that supports MED is discovered.
- Selected Optional TLVs—Select the TLVs that can be published by the device by moving them from the Available Optional TLVs list to the Selected Optional TLVs list.
- Selected Network Policies—Select the LLDP MED policies to be published by LLDP by moving them from the Available Network Policies list to the Selected Network Policies list. To include one or more user-defined network policies in the advertisement, you must also select **Network Policy** from the Available Optional TLVs.

Note
The following fields must be entered in hexadecimal characters in the exact data format that is defined in the LLDP-MED standard (ANSI-TIA-1057_final_for_publication.pdf):

- Location Coordinate—Enter the coordinate location to be published by LLDP.
- Location Civic Address—Enter the civic address to be published by LLDP.
- Location ECS ELIN—Enter the Emergency Call Service (ECS) ELIN location to be published by LLDP.

Step 5 Click **Apply**. The LLDP MED port settings are written to the Running Configuration file.

LLDP Port Status

The LLDP Port Status page contains the LLDP global information for every port.

Procedure

Step 1 To view the LLDP port status, click **Administration** > **Discovery - LLDP** > **LLDP Port Status**.

Information for all ports is displayed.

Step 2 Select a specific port and click **LLDP Local Information Detail** to see the details of the LLDP and LLDP-MED TLVs sent out to the port.

Step 3 Select a specific port and click **LLDP Neighbor Information Detail** to see the details of the LLDP and LLDP-MED TLVs received from the port.

LLDP Port Status Global Information

- Chassis ID Subtype—Type of chassis ID (for example, MAC address).
- Chassis ID—Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the device appears.
- System Name—Name of device.
- System Description—Description of the device (in alpha-numeric format).
- Supported System Capabilities—Primary functions of the device, such as Bridge, WLAN AP, or Router.

- Enabled System Capabilities—Primary enabled function(s) of the device.
- Port ID Subtype—Type of the port identifier that is shown.

LLDP Port Status Table

- Interface—Port identifier.
- LLDP Status—LLDP publishing option.
- LLDP MED Status—Enabled or disabled.
- Local PoE ((Power Type, Power Source, Power Priority, Power Value)—Local PoE information advertised.
- Remote PoE (Power Type, Power Source, Power Priority, Power Value)—PoE information advertised by the neighbor.
- # of neighbors—Number of neighbors discovered.
- Neighbor capability of 1st device—Displays the primary functions of the neighbor; for example: Bridge or Router.

LLDP Local Information

To view the LLDP local port status advertised on a port, follow these steps:

Procedure

Step 1 Click **Administration** > **Discovery - LLDP** > **LLDP Local Information**.

Step 2 Select the interface and port for which the LLDP local information is to be displayed.

The LLDP Local Information page contains the following fields:

Global

- Chassis ID Subtype—Type of chassis ID. (For example, the MAC address.)
- Chassis ID—Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the device appears.
- System Name—Name of device.
- System Description—Description of the device (in alpha-numeric format).
- Supported System Capabilities—Primary functions of the device, such as Bridge, WLAN AP, or Router.
- Enabled System Capabilities—Primary enabled function(s) of the device.
- Port ID Subtype—Type of the port identifier that is shown.
- Port ID—Identifier of port.
- Port Description—Information about the port, including manufacturer, product name and hardware/software version.

Management Address

- IPv4 Address—IPv4 returned address most appropriate for management use.
- IPv6 Global Address—IPv6 returned global address most appropriate for management use.
- IPv6 Link Local Address—IPv6 returned link local address most appropriate for management use.

MAC/PHY Details

- Auto-Negotiation Supported—Port speed auto-negotiation support status. The possible values are True and False.
- Auto-Negotiation Enabled—Port speed auto-negotiation active status. The possible values are True and False.
- Auto-Negotiation Advertised Capabilities—Port speed auto-negotiation capabilities, for example, 1000BASE-T half duplex mode, 100BASE-TX full duplex mode.
- Operational MAU Type—Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network; for example, 100BASE-TX full duplex mode.

802.3 Details

- 802.3 Maximum Frame Size - The maximum supported IEEE 802.3 frame size.

802.3 Link Aggregation

- Aggregation Capability—Indicates whether the interface can be aggregated.
- Aggregation Status—Indicates whether the interface is aggregated.
- Aggregation Port ID—Advertised aggregated interface ID.

802.3 Energy Efficient Ethernet (EEE)

- Local Tx—Indicates the local link partner's reflection of the remote link partner's Tx value.
- Local Rx—Indicates the local link partner's reflection of the remote link partner's Rx value.
- Remote Tx Echo—Indicates the time (in micro seconds) that the transmitting link partner waits before it starts transmitting data after leaving Low Power Idle (LPI mode).
- Remote Rx Echo—Indicates the time (in micro seconds) that the receiving link partner requests that the transmitting link partner waits before transmission of data following Low Power Idle (LPI mode).

802.3 Power via MDI

- MDI Power Support Port Class—Advertised power support port class.
- PSE MDI Power Support—Indicates if MDI power is supported on the port.
- PSE MDI Power State—Indicates if MDI power is enabled on the port.
- PSE Power Pair Control Ability—Indicates if power pair control is supported on the port.
- PSE Power Pair—Power pair control type supported on the port.
- PSE Power Class—Advertised power class of the port.
- Power Type—Type of pod device connected to the port.
- Power Source—Port power source.

- Power Priority—Port power priority
- PD Requested Power Value—Amount of power allocated by the PSE to the PD.
- PSE Allocated Power Value—Amount of power allocated to the sourcing equipment (PSE).

4-Wire Power via MDI

- 4-Pair PoE Supported—Indicates system and port support enabling the 4-pair wire (true only for specific ports that have this HW ability).
- Spare Pair Detection/Classification Required—Indicates that the 4-pair wire is needed.
- PD Spare Pair Desired State—Indicates a pod device requesting to enable the 4-pair ability.
- PD Spare Pair Operational State—Indicates if the 4-pair ability is enabled or disabled.

MED Details

- Capabilities Supported—MED capabilities enabled on the port.
- Current Capabilities—MED TLVs advertised by the port.
- Device Class—LLDP-MED endpoint device class. The possible device classes are:
  - Endpoint Class 1—Indicates a generic endpoint class, offering basic LLDP services.
  - Endpoint Class 2—Indicates a media endpoint class, offering media streaming capabilities as well as all Class 1 features.
  - Endpoint Class 3—Indicates a communications device class, offering all Class 1 and Class 2 features plus location, 911, Layer 2 switch support and device information management capabilities.
- PoE Device Type—Port PoE type, for example, PD/PSE.
- PoE Power Source—Port's power source.
- PoE Power Priority—Port's power priority.
- PoE Power Value—Port's power value.
- Hardware Revision –Hardware version.
- Firmware Revision—Firmware version.
- Software Revision—Software version.
- Serial Number—Device serial number.
- Manufacturer Name—Device manufacturer name.
- Model Name—Device model name.
- Asset ID—Asset ID.

Location Information

Enter the following data structures in hexadecimal as described in section 10.2.4 of the ANSI-TIA-1057 standard:

- Civic—Civic or street address.

- Coordinates—Location map coordinates—latitude, longitude, and altitude.
- ECS ELIN—Device's Emergency Call Service (ECS) Emergency Location Identification Number (ELIN).

Network Policy Table

- Application Type—Network policy application type, for example, Voice.
- VLAN ID—VLAN ID for which the network policy is defined.
- VLAN Type—VLAN type, Tagged or Untagged, for which the network policy is defined.
- User Priority—Network policy user priority.
- DSCP—Network policy DSCP.

LLDP Neighbor Information

The LLDP Neighbor Information page contains information that was received from neighboring devices. After timeout (based on the value received from the neighbor Time To Live TLV during which no LLDP PDU was received from a neighbor), the information is deleted.

To view the LLDP neighbors information, follow these steps:

Procedure

Step 1 Click **Administration** > **Discovery - LLDP** > **LLDP Neighbor Information**.

Step 2 Select the interface for which LLDP neighbor information is to be displayed.

This page displays the following fields for the selected interface:

- Local Port—Number of the local port to which the neighbor is connected.
- Chassis ID Subtype—Type of chassis ID (for example, MAC address).
- Chassis ID—Identifier of the 802 LAN neighboring device's chassis.
- Port ID Subtype—Type of the port identifier that is shown.
- Port ID—Identifier of port.
- System Name—Published name of the device.
- Time to Live—Time interval (in seconds) after which the information for this neighbor is deleted.

Step 3 Select a local port, and click **Details**.

The LLDP Neighbor Information page contains the following fields:

Port Details

- Local Port—Port number.
- MSAP Entry—Device Media Service Access Point (MSAP) entry number.

Basic Details

- Chassis ID Subtype—Type of chassis ID (for example, MAC address).
- Chassis ID—Identifier of the 802 LAN neighboring device chassis.
- Port ID Subtype—Type of the port identifier that is shown.
- Port ID—Identifier of port.
- Port Description—Information about the port, including manufacturer, product name and hardware/software version.
- System Name—Name of system that is published.
- System Description—Description of the network entity (in alpha-numeric format). This includes the system name and versions of the hardware, operating system, and networking software supported by the device. The value equals the sysDescr object.
- Supported System Capabilities—Primary functions of the device. The capabilities are indicated by two octets. Bits 0 through 7 indicate Other, Repeater, Bridge, WLAN AP, Router, Telephone, DOCSIS cable device, and station, respectively. Bits 8 through 15 are reserved.
- Enabled System Capabilities—Primary enabled function(s) of the device.

Management Address Table

- Address Subtype—Managed address subtype; for example, MAC or IPv4.
- Address—Managed address.
- Interface Subtype—Port subtype.
- Interface Number—Port number.

MAC/PHY Details

- Auto-Negotiation Supported—Port speed auto-negotiation support status. The possible values are True and False.
- Auto-Negotiation Enabled—Port speed auto-negotiation active status. The possible values are True and False.
- Auto-Negotiation Advertised Capabilities—Port speed auto-negotiation capabilities, for example, 1000BASE-T half duplex mode, 100BASE-TX full duplex mode.
- Operational MAU Type—Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network; for example, 100BASE-TX full duplex mode.

802.3 Power via MDI

- MDI Power Support Port Class—Advertised power support port class.
- PSE MDI Power Support—Indicates if MDI power is supported on the port.
- PSE MDI Power State—Indicates if MDI power is enabled on the port.
- PSE Power Pair Control Ability—Indicates if power pair control is supported on the port.
- PSE Power Pair—Power pair control type supported on the port.
- PSE Power Class—Advertised power class of the port.

- Power Type—Type of pod device connected to the port.
- Power Source— Port power source.
- Power Priority—Port power priority.
- PD Requested Power Value—Amount of power requested by the pod device.
- PSE Allocated Power Value—Amount of power allocated by the PSE to the PD.

4-Wire Power via MDI

- 4-Pair PoE Supported—Indicates system and port support enabling the 4-pair wire (true only for specific ports that have this HW ability).
- Spare Pair Detection/Classification Required—Indicates that the 4-pair wire is needed.
- PD Spare Pair Desired State—Indicates a pod device requesting to enable the 4-pair ability.
- PD Spare Pair Operational State—Indicates if the 4-pair ability is enabled or disabled.

802.3 Details

- 802.3 Maximum Frame Size—Advertised maximum frame size that is supported on the port.

802.3 Link Aggregation

- Aggregation Capability—Indicates if the port can be aggregated.
- Aggregation Status—Indicates if the port is currently aggregated.
- Aggregation Port ID—Advertised aggregated port ID.

802.3 Energy Efficient Ethernet (EEE)

- Remote Tx—Indicates the time (in micro seconds) that the transmitting link partner waits before it starts transmitting data after leaving Low Power Idle (LPI mode).
- Remote Rx—Indicates the time (in micro seconds) that the receiving link partner requests that the transmitting link partner waits before transmission of data following Low Power Idle (LPI mode).
- Local Tx Echo—Indicates the local link partner’s reflection of the remote link partner’s Tx value.
- Local Rx Echo—Indicates the local link partner’s reflection of the remote link partner’s Rx value.

MED Details

- Capabilities Supported—MED capabilities enabled on the port.
- Current Capabilities—MED TLVs advertised by the port.
- Device Class—LLDP-MED endpoint device class. The possible device classes are:
  - Endpoint Class 1—Indicates a generic endpoint class, offering basic LLDP services.
  - Endpoint Class 2—Indicates a media endpoint class, offering media streaming capabilities as well as all Class 1 features.
  - Endpoint Class 3—Indicates a communications device class, offering all Class 1 and Class 2 features plus location, 911, Layer 2 switch support and device information management capabilities.

- PoE Device Type—Port PoE type, for example, PD/PSE.
- PoE Power Source—Port's power source.
- PoE Power Priority—Port's power priority.
- PoE Power Value—Port's power value.
- Hardware Revision –Hardware version.
- Firmware Revision—Firmware version.
- Software Revision—Software version.
- Serial Number—Device serial number.
- Manufacturer Name—Device manufacturer name.
- Model Name—Device model name.
- Asset ID—Asset ID.

802.1 VLAN and Protocol

- PVID—Advertised port VLAN ID.

PPVID Table

- VID—Protocol VLAN ID.
- Supported—Supported Port and Protocol VLAN IDs.
- Enabled—Enabled Port and Protocol VLAN IDs.

VLAN ID Table

- VID—Port and Protocol VLAN ID.
- VLAN Name—Advertised VLAN names.

Protocol ID Table

- Protocol ID—Advertised protocol IDs.

Location Information

Enter the following data structures in hexadecimal as described in section 10.2.4 of the ANSI-TIA-1057 standard:

- Civic—Civic or street address.
- Coordinates—Location map coordinates—latitude, longitude, and altitude.
- ECS ELIN—Device's Emergency Call Service (ECS) Emergency Location Identification Number (ELIN).
- Unknown—Unknown location information.

Network Policy Table

- Application Type—Network policy application type, for example, Voice.
- VLAN ID—VLAN ID for which the network policy is defined.

- VLAN Type—VLAN type, Tagged or Untagged, for which the network policy is defined.
- User Priority—Network policy user priority.
- DSCP—Network policy DSCP.

LLDP Statistics

The LLDP Statistics page displays LLDP statistical information per port.

To view the LLDP statistics, follow these steps:

Procedure

Step 1 Click **Administration** > **Discovery - LLDP** > **LLDP Statistics**.

For each port, the fields are displayed:

- Interface—Identifier of interface.
- Tx Frames (Total)—Number of transmitted frames.
- Rx Frames
  - Total—Number of received frames
  - Discarded—Total number of received frames that discarded
  - Errors—Total number of received frames with errors
- Rx TLVs
  - Discarded—Total number of received TLVs that discarded
  - Unrecognized—Total number of received TLVs that unrecognized.
- Neighbor's Information Deletion Count—Number of neighbor ageouts on the interface.

Step 2 Click **Refresh** to view the latest statistics.

LLDP Overloading

Note This setting is only available in the Advanced Mode view.)

LLDP adds information as LLDP and LLDP-MED TLVs into the LLDP packets. LLDP overload occurs when the total amount of information to be included in an LLDP packet exceeds the maximum PDU size supported by an interface.

The LLDP Overloading page displays the number of bytes of LLDP/LLDP-MED information, the number of available bytes, and the overloading status of every interface.

To view LLDP overloading information:

Procedure

Step 1 Click **Administration** > **Discovery - LLDP** > **LLDP Overloading**.

In the LLDP Overloading Table, the following information is displayed for each port:

- Interface—Port identifier.
- Total Bytes In-Use—Total number of bytes of LLDP information in each packet
- Available Bytes Left—Total amount of available bytes left for other LLDP information in each packet.
- Status—Whether TLVs are being transmitted or if they are overloaded.

Step 2 To view the overloading details for a port, select it and click **Details**.

This page contains the following information for each TLV sent on the port:

- LLDP Mandatory TLVs
  - Size (Bytes)—Total mandatory TLV byte size
  - Status—If the mandatory TLV group is being transmitted, or if the TLV group was overloaded.
- LLDP MED Capabilities
  - Size (Bytes)—Total LLDP MED capabilities packets byte size
  - Status—If the LLDP MED capabilities packets sent, or if they overloaded.
- LLDP MED Location
  - Size (Bytes)—Total LLDP MED location packets byte size
  - Status—If the LLDP MED locations packets sent, or if they overloaded.
- LLDP MED Network Policy
  - Size (Bytes)—Total LLDP MED network policies packets byte size
  - Status—If the LLDP MED network policies packets sent, or if they overloaded.
- LLDP MED Extended Power via MDI
  - Size (Bytes)—Total LLDP MED extended power via MDI packets byte size.
  - Status—If the LLDP MED extended power via MDI packets sent, or if they overloaded.

- 802.3 TLVs
  - Size (Bytes)—Total LLDP MED 802.3 TLVs packets byte size.
  - Status—If the LLDP MED 802.3 TLVs packets sent, or if they overloaded.
- LLDP Optional TLVs
  - Size (Bytes)—Total LLDP MED optional TLVs packets byte size.
  - Status—If the LLDP MED optional TLVs packets sent, or if they overloaded.
- LLDP MED Inventory
  - Size (Bytes)—Total LLDP MED inventory TLVs packets byte size.
  - Status—If the LLDP MED inventory packets sent, or if they overloaded.
- Total
  - Total (Bytes)—Total number of bytes of LLDP information in each packet.
  - Available Bytes Left—Total number of available bytes left to send for additional LLDP information in each packet.

Discovery - CDP

Cisco Discovery Protocol is a Layer 2, media-independent, and network-independent protocol that networking applications use to learn about nearby, directly connected devices. Cisco Discovery Protocol is enabled by default. Each device configured for Cisco Discovery Protocol advertises at least one address at which the device can receive messages and sends periodic advertisements (messages) to the well-known multicast address 01:00:0C:CC:CC:CC. Devices discover each other by listening at that address. They also listen to messages to learn when interfaces on other devices are up or go down.

Advertisements contain time-to-live information, which indicates the length of time a receiving device should hold Cisco Discovery Protocol information before discarding it. Advertisements supported and configured in Cisco software are sent, by default, every 60 seconds on interfaces that support Subnetwork Access Protocol (SNAP) headers. Cisco devices never forward Cisco Discovery Protocol packets. Cisco devices that support Cisco Discovery Protocol store the information received in a table. Information in this table is refreshed every time an advertisement is received, and information about a device is discarded after three advertisements from that device are missed.

This section describes how to configure CDP.

Properties

Similar to LLDP, the Cisco Discovery Protocol (CDP) is a link layer protocol for directlyconnected neighbors to advertise themselves and their capabilities to each other. Unlike LLDP, CDP is a Cisco proprietary protocol.To configure the CDP properties, complete the following steps:

Procedure

Step 1 Click **Administration** > **Discovery - CDP** > **Properties**.

Step 2 Enter the parameters.

CDP Status	Select to enable CDP on the device.
CDP Frames Handling	If CDP is not enabled, select the action to be taken if a packet that matches the selected criteria is received: • Bridging—Forward the packet based on the VLAN • Filtering—Delete the packet • Flooding—VLAN unaware flooding that forwards incoming CDP packets to all the ports excluding the ingress ports.
CDP Voice VLAN Advertisement	Select to enable the device to advertise the voice VLAN in CDP on all of the ports that are CDP enabled, and are member of the voice VLAN. The voice VLAN is configured in the Properties, on page 156.
CDP Mandatory TLVs Validation	If selected, incoming CDP packets not containing the mandatory TLVs are discarded and the invalid error counter is incremented.
CDP Version	Select the version of CDP to use.
CDP Hold Time	Amount of time that CDP packets are held before the packets are discarded, measured in multiples of the TLV Advertise Interval. For example, if the TLV Advertise Interval is 30 seconds, and the Hold Multiplier is 4, then the LLDP packets are discarded after 120 seconds. The following options are possible: • Use Default—Use the default time (180 seconds) • User Defined—Enter the time in seconds.
CDP Transmission Rate	The rate in seconds at which CDP advertisement updates are sent. The following options are possible: • Use Default—Use the default rate (60 seconds) • User Defined—Enter the rate in seconds.
Device ID Format	Select the format of the device ID (MAC address or serial number). The following options are possible: • Use Default—Use the default rate (60 seconds) • User Defined—Enter the rate in seconds.

Source Interface	IP address to be used in the TLV of the frames. The following options are possible: • Use Default—Use the IP address of the outgoing interface. • User Defined—Use the IP address of the interface (in the Interface field) in the address TLV.
Interface	IF User Defined was selected for Source Interface, select the interface.
Syslog Voice VLAN Mismatch	Check to send a SYSLOG message when a voice VLAN mismatch is detected. This means that the voice VLAN information in the incoming frame does not match what the local device is advertising.
Syslog Native VLAN Mismatch	Check to send a SYSLOG message when a native VLAN mismatch is detected. This means that the native VLAN information in the incoming frame does not match what the local device is advertising.
Syslog Duplex Mismatch	Check to send a SYSLOG message when duplex information is mismatched. This means that the duplex information in the incoming frame does not match what the local device is advertising.

Step 3 Click **Apply**. The LLDP properties are defined.

Interface Settings

Note This setting is only available in the Advanced Mode view.

The Interface Settings page enables you to enable/disable CDP per port. By setting these properties, it's possible to select the types of information to be provided to devices that support the LLDP protocol.

The LLDP-MED TLVs to be advertised can be selected in the LLDP MED Port Settings, on page 97.

To define the CDP interface settings:

Procedure

Step 1 Click **Administration** > **Discovery - CDP** > **Interface Settings**.

This page displays the following CDP information for each interface.

- CDP Status—CDP publishing option for the port.
- Reporting Conflicts with CDP Neighbors—Status of the reporting options that are enabled/disabled in the Edit page (Voice VLAN/Native VLAN/Duplex).
- No. of Neighbors—Number of neighbors detected.

The bottom of the page has four buttons:

- Copy Settings—Select to copy a configuration from one port to another.
- Edit—Fields explained in Step 2 below.
- CDP Local Information Details—Takes you to the CDP Local Information, on page 111 .
- CDP Neighbor Information Details—Takes you to the CDP Neighbors Information, on page 113.

Step 2 Select a port and click **Edit.**

This page provides the following fields:

- Interface—Select the interface to be defined.
- CDP Status—Select to enable/disable the CDP publishing option for the port.

Note
The next three fields are operational when the device has been set up to send traps to the management station.

- Syslog Voice VLAN Mismatch—Select to enable sending a SYSLOG message when a voice VLAN mismatch is detected. This means that the voice VLAN information in the incoming frame doesn't match what the local device is advertising.
- Syslog Native VLAN Mismatch—Select to enable sending a SYSLOG message when a native VLAN mismatch is detected. This means that the native VLAN information in the incoming frame doesn't match what the local device is advertising.
- Syslog Duplex Mismatch—Select to enable sending a SYSLOG message when duplex information mismatch is detected. This means that the duplex information in the incoming frame doesn't match what the local device is advertising.

Step 3 Enter the relevant information, and click **Apply**. The port settings are written to the Running Configuration.

CDP Local Information

To view information that is advertised by the CDP protocol about the local device:

Procedure

Click Administration > **Discovery - CDP** > **CDP Local Information**. The following fields are displayed:

Interface	Number of the local port.
CDP State	Displays whether CDP is enabled or not.
Device ID TLV	• Device ID Type—Type of the device ID advertised in the device ID TLV • Device ID—Device ID advertised in the device ID TLV
System Name TLV	System Name—System name of the device.

Address TLV	Address1-3—IP addresses (advertised in the device address TLV).
Port TLV	Port ID—Identifier of port advertised in the port TLV.
Port ID	Identifier of port advertised in the port TLV.
Capabilities TLV	Capabilities—Capabilities advertised in the port TLV).
Version TLV	Version—Information about the software release on which the device is running.
Platform TLV	Platform—Identifier of platform advertised in the platform TLV.
Native VLAN TLV	Native VLAN—The native VLAN identifier advertised in the native VLAN TLV.
Full/Half Duplex TLV	Duplex—Whether port is half or full-duplex advertised in the full/half duplex TLV.
Appliance TLV	• Appliance ID—Type of device attached to port advertised in the appliance TLV • Appliance VLAN ID—VLAN on the device used by the appliance, for instance if the appliance is an IP phone, this is the voice VLAN.
Extended Trust TLV	Extended Trust—Enabled indicates that the port is trusted, and the packets received are marked. In this case, packets received on such a port aren't re-marked. Disabled indicates that the port isn't trusted in which case, the following field is relevant.
CoS for Untrusted Ports TLV	CoS for Untrusted Ports—If Extended Trust is disabled on the port, this field displays the Layer 2 CoS value, meaning, an 802.1D/802.1p priority value. This is the COS value with which all packets received on an untrusted port are remarked by the device.
Power Available TLV	• Request ID—Last power request ID received echoes the Request-ID field last received in a Power Requested TLV. It's 0 if no Power Requested TLV was received since the interface last transitioned to Up. • Power Management ID—Value incremented by 1 (or 2, to avoid 0) each time any one of the following events occurs: Available-Power or Management Power Level change A Power Requested TLV is received with a Request-ID that is different from the last-received set. The interface transitions to Down. • Available Power—Amount of power consumed by port • Management Power Level—Displays the supplier's request to the pod device for its Power Consumption TLV. The device always displays "No Preference" in this field.

4-Wire Power via MDI (UPOE) TLV	Displays whether this TLV is supported. • 4-Pair PoE Supported—Displays whether PoE is supported. • Spare Pair Detection/Classification Required—Displays whether this classification is required. • PD Spare Pair Desired State—Displays the PD spare pair desired state. • PD Spare Pair Operational State—Displays the PSE spare pair state.

CDP Neighbors Information

The CDP Neighbors Information page displays CDP information received from neighboring devices.

Information is deleted, after timeout (based on the value received from Time To Live TLV during which no CDP PDU was received).

To view the CDP neighbors information, proceed as follows:

Procedure

Step 1 Click **Administration** > **Discovery - CDP** > **CDP Neighbor Information**.

Step 2 To select a filter, check the Filter checkbox, select a Local interface, and click **Go**.

The filter is applied on the list, and Clear Filter is activated to enable stopping the filter.

The CDP Neighbor Information page contains the following fields for the link partner (neighbor):

Device ID	Neighbors device ID.
System Name	Neighbors system name.
Local Interface	Number of the local port to which the neighbor is connected.
Advertisement Version	CDP protocol version.
Time to Live	Time interval (in seconds) after which the information for this neighbor is deleted.
Capabilities	Capabilities advertised by neighbor.
Platform	Information from Platform TLV of neighbor.
Neighbor Interface	Outgoing interface of the neighbor.

Step 3 Select a device, and click **Details**.

This page contains the following fields about the neighbor (actual field display depends on what the neighbor is advertising):

Device ID	Neighbors device ID.

System Name	Neighbors system name.
Local Interface	Number of the local port to which the neighbor is connected.
Advertisement Version	CDP protocol version.
Time to Live (sec)	Time interval (in seconds) after which the information for this neighbor is deleted.
Capabilities	Capabilities advertised by neighbor.
Platform	Information from Platform TLV of neighbor.
Neighbor Interface	Outgoing interface of the neighbor.
Native VLAN	Neighbors native VLAN.
Duplex	Whether neighbors interface is half or full-duplex.
Addresses	Neighbors addresses.
Power Drawn	Amount of power consumed by neighbor on the interface.
Version	Neighbors software version.
Power Request	Power requested by PD that is connected to the port. • Power Request List—Each PD may send a list (up to 3) of supported power levels.
Power Available	Shown if a PSE is connected to the port.

Note Disconnects on the Clear Table button all connected devices if from CDP, and if Auto Smartport is enabled change all port types to default.

CDP Statistics

The CDP Statistics page displays information regarding CDP frames that sent or received from a port. CDP packets are received from devices attached to the switches interfaces, and are used for the Smartport feature.

To view CDP statistics, follow these steps:

Procedure

Step 1 Click **Administration** > **Discovery - CDP** > **CDP Statistics.**

The following fields are displayed for every interface:

Packets Received/Packets Transmitted:

- Version 1—Number of CDP version 1 packets received/transmitted.
- Version 2—Number of CDP version 2 packets received/transmitted.
- Total—Total number of CDP packets received/transmitted.

CDP Error Statistics:

- Illegal Checksum—Number of packets received with illegal checksum value.
- Other Errors—Number of packets received with errors other than illegal checksums.
- Neighbors Over Maximum—Number of times that packet information couldn't be stored in cache because of lack of room.

Step 2 To clear all counters on all interfaces, click **Clear All Interface Counters**. To clear all counters on an interface, select it and click **Clear Interface Counters**.

Locate Device

This feature enables flashing all network port LEDs on a specific device in the network to locate the device physically. This feature is useful for locating a device within a room with many interconnected devices. When this feature is activated, all network port LEDs on the device flash for a configured duration (one minute by default).

Procedure

Step 1 Click **Administration** > **Locate Device**.

Step 2 Enter values in the following fields:

- Duration—Enter for how long (in seconds) the port's LEDs flash.
- Remaining Time—This field is only displayed if the feature is currently activated. It displays the remaining time during which the LED flashes.
- Unit ID—This field is only displayed when the device is in a stack. Specify the unit on which the network port LEDs flash or All for all units.

Step 3 Click **Start** to activate the feature.

When the feature is activated the Start button is replaced by the Stop button, which allows you to stop the LED blinking before the defined timer expires.

Ping

The Ping utility tests if a remote host can be reached and measures the round-trip time for packets sent.

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response, sometimes called a pong. It measures the round-trip time and records any packet loss.

To ping a host, follow these steps:

Procedure

Step 1 Click **Administration** > **Ping**.

Step 2 Configure ping by entering the fields:

Option	Description
Host Definition	Select whether to specify the source interface by its IP address or name. This field influences the interfaces that are displayed in the Source IP field, as described below.
IP Version	If the source interface is identified by its IP address, select either IPv4 or IPv6 to indicate that it will be entered in the selected format.
Source IP	Select the source interface as the source IPv4 address for communication with the destination. If the Host Definition field was By Name, all IPv4 and IPv6 addresses are displayed. If the Host Definition field was By IP Address, only the existing IP addresses of the type specified in the IP Version field are displayed. **Note** If the Auto option is selected, the system computes the source address based on the destination address.
Destination IPv6 Address Type	Select one of the following options: • Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration. • Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
Link Local Interface	If the IPv6 address type is Link Local, select from where it is received.
Destination IP Address/Name	Address or host name of the device to be pinged. Whether this is an IP address or host name depends on the Host Definition.
Ping Interval **Note** This setting is only available in the Advanced Mode view.	Length of time the system waits between ping packets. Ping is repeated the number of times configured in the Number of Pings fields, whether the ping succeeds or not. Select to use the default interval or specify your own value.
Number of Pings **Note**	The number of times the ping operation is performed. Select to use the default or specify your own value.

Option	Description
This setting is only available in the Advanced Mode view.	
Status	Displays whether the ping succeeded or failed.

Step 3 Click **Activate Ping** to ping the host. The ping status appears and a message is added to the list of messages, indicating the result of the ping operation.

Step 4 View the results of ping in the Ping Counters and Status section of the page:

- Number of Sent Packets—Number of packets sent by ping
- Number of Received Packets—Number of packets received by ping
- Packet Loss—Percentage of packets lost in ping process
- Minimum Round Trip Time—Shortest time for packet to return
- Maximum Round Trip Time—Longest time for packet to return
- Average Round Trip Time—Average time for packet to return
- Status—Fail or succeed

Traceroute

Traceroute discovers the IP routes forwarded by sending an IP packet to the target host and back to the device. The Traceroute page shows each hop between the device and a target host, and the round-trip time to each such hop.

Procedure

Step 1 Click **Administration** > **Traceroute**.

Step 2 Configure Traceroute by entering information in the following fields:

- Host Definition—Select whether hosts are identified by their IP address or name.
- IP Version—If the host is identified by its IP address, select either IPv4 or IPv6 to indicate that it will be entered in the selected format.
- Source IP—Select the source interface whose IPv4 address will be used as the source IPv4 address for communication messages. If the Host Definition field was By Name, all IPv4 and IPv6 addresses are displayed in this drop-down field. If the Host Definition field was By IP Address, only the existing IP addresses of the type specified in the IP Version field will be displayed.
- Host IP Address/Name—Enter the host address or name.

- TTL—Enter the maximum number of hops that Traceroute permits. This is used to prevent a case where the sent frame gets into an endless loop. The Traceroute command terminates when the destination is reached or when this value is reached. To use the default value (30), select **Use Default**.

  Note
  This setting is only available in the Advanced Mode view.

- Timeout—Enter the length of time that the system waits for a frame to return before declaring it lost, or select **Use Default**.

  Note
  This setting is only available in the Advanced Mode view.

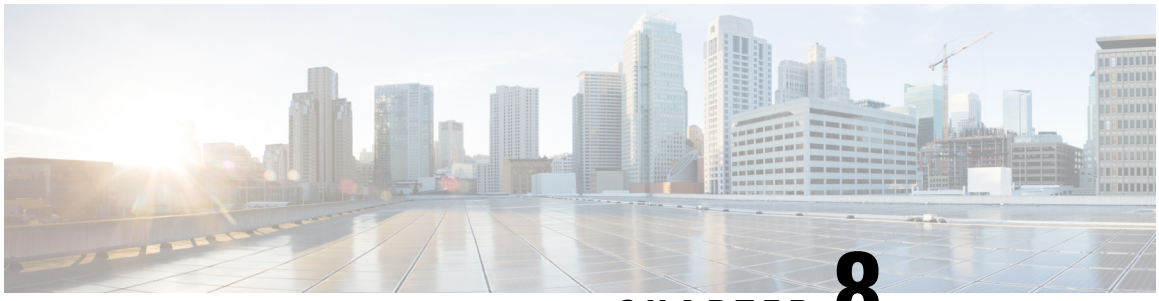
Step 3 Click **Activate Traceroute**. The operation is performed.

Note
A pop-up will appear indicating if you would like to stop the traceroute. Click **Stop Traceroute** to stop the process.

A page appears to show the Round Trip Time (RTT) and status for each trip in the fields:

- Index—Displays the number of the hop.
- Host—Displays a stop along the route to the destination.

  Round Trip Time (1-3)—Displays the round trip Time (ms) and Status.



CHAPTER 8

Port Management

This chapter contains the following sections:

- Port Settings, on page 119
- Error Recovery Settings, on page 122
- Loopback Detection Settings, on page 123
- Link Aggregation, on page 124
- UDLD, on page 127
- PoE, on page 130
- Green Ethernet, on page 135

Port Settings

The Port Settings page displays the global and per port setting of all the ports. Here, you can select and configure the desired ports from the Edit Port Settings page.

To configure port settings, follow these steps:

Procedure

Step 1 Click **Port Management** > **Port Settings**.

The port settings are displayed for all ports.

Step 2 Enter the following fields:

- Link Flap Prevention—Select to minimize the disruption to your network. Enabled, this command automatically disables ports that experience link-flap events.
- Jumbo Frames—Check to support packets of up to 9 KB in size. If Jumbo Frames isn't enabled (default), the system supports packet size up to 2,000 bytes. Note that receiving packets bigger than 9 KB might cause the receiving port to shut down. Also, sending packets bigger than 10 KB bytes might cause the receiving port to shutdown.

  For jumbo frames to take effect, the device must be rebooted after the feature is enabled.

Step 3 Click **Apply** to update the global setting.

Jumbo frames configuration changes take effect only after the Running Configuration is explicitly saved to the Startup Configuration File using the File Operations, on page 76, and the device is rebooted.

Step 4 To update the port settings, select the desired port, and click **Edit.**

Step 5 Modify the following parameters:

Interface	Select the port number.
Port Description	Enter the port user-defined name or comment. **Note** The Interface and Port Description are displayed on the main page in the Port column.
Port Type	Displays the port type and speed. The possible options are: • Copper Ports—Regular, not Combo, support the following values: 10M, 100M, 1000M (type: Copper) and 10G, 2.5G, 5G and 10G. • Combo Ports —Combo port connected with either copper CAT6a cable or SFP Fiber Gigabit Interface • 10G-Fiber Optics—Ports with speed of either 1G or 10G
Administrative Status	Select whether the port must be Up or Down when the device is rebooted.
Operational Status	Displays whether the port is currently Up or Down. If the port is down because of an error, the description of the error is displayed
Link Status SNMP Traps	Select to enable generation of SNMP traps that notify of changes to the link status of the port.
Time Range	Select to enable the time range during which the port is in Up state. When the time range isn't active, the port is in shutdown. If a time range is configured, it is effective only when the port is administratively Up.
Time Range Name	Select the profile that specifies the time range. Not relevant for the OOB port. If a time range isn't yet defined, click **Edit**.
Operational Time Range State	Range State—Displays whether the time range is currently active or inactive.
Auto Negotiation	Select to enable auto-negotiation on the port. Auto-negotiation enables a port to advertise its transmission speed, duplex mode, and Flow Control abilities to the port link partner.
Operational Auto Negotiation	Displays the current auto-negotiation status on the port.
Administrative Port Speed	Select the speed of the port. The port type determines the available speeds. You can designate Administrative Speed only when port auto-negotiation is disabled.
Operational Port Speed	Displays the current port speed that is the result of negotiation.

Administrative Duplex Mode	Select the port duplex mode. This field is configurable only when auto-negotiation is disabled, and the port speed is set to 10M or 100M. At port speed of 1G, the mode is always full-duplex. The possible options are: • Half—The interface supports transmission between the device and the client in only one direction at a time. • Full—The interface supports transmission between the device and the client in both directions simultaneously.
Operational Duplex Mode	Displays the ports current duplex mode.
Auto Advertisement	Select the capabilities advertised by auto-negotiation when it is enabled. **Note** Not all options are relevant for all devices. The options are: • Max Capability—All port speeds and duplex mode settings can be accepted. • 10 Half—10 Mbps speed and Half Duplex mode (doesn't appear on XG devices) • 10 Full—10 Mbps speed and Full Duplex mode (doesn't appear on XG devices) • 100 Half—100 Mbps speed and Half Duplex mode (doesn't appear on XG devices) • 100 Full—100 Mbps speed and Full Duplex mode • 1000 Full—1000 Mbps speed and Full Duplex mode
Operational Advertisement	Displays the capabilities currently published to the ports neighbor. The possible options are those specified in the Administrative Advertisement field.
Preference Mode	Available only if auto-negotiation is enabled. Select the active-member mode of the interface for the auto-negotiation operation. Select one of the following options: • Member—Begin negotiation with the preference that the device port is the member in the auto-negotiation process. • Active—Begin negotiation with the preference that the device port is the active in the auto-negotiation process.
Neighbor Advertisement	Displays the capabilities advertised by the neighboring device.
Back Pressure	Select the Back Pressure mode on the port (used with Half Duplex mode) to slow down the packet reception speed when the device is congested. Selecting this option disables the remote port, preventing it from sending packets by jamming the signal.
Flow Control	Enable or disable 802.3x Flow Control, or enable the auto-negotiation of Flow Control on the port (only when in Full Duplex mode). Flow control auto-negotiation can't be enabled on combo ports.

MDI/MDIX-Media Dependent Interface (MDI)/Media Dependent Interface with Crossover (MDIX) status on the port.	The options are: • MDIX—Select to swap the port's transmit and receive pairs. • MDI—Select to connect this device to a station by using a straight through cable. • Auto-Select to configure this device to automatically detect the correct pinouts for connection to another device.
Operational MDI/MDIX	Displays the current MDI/MDIX setting.
Protected Port	Select to make this a protected port. (A protected port is also referred as a Private VLAN Edge (PVE).) The features of a protected port are as follows: • Protected Ports provide Layer 2 isolation between interfaces (Ethernet ports and LAGs) that share the same VLAN. • Packets received from protected ports can be forwarded only to unprotected egress ports. Protected port filtering rules are also applied to packets that are forwarded by software, such as snooping applications. • Port protection is not subject to VLAN membership. Devices connected to protected ports are not allowed to communicate with each other, even if they are members of the same VLAN. • Both ports and LAGs can be defined as protected or unprotected. Protected LAGs are described in LAG Settings, on page 125.
Member in LAG	If the port is a member of a LAG, the LAG number appears; otherwise this field is left blank.

Step 6 Click **Apply**. The Port Settings are written to the Running Configuration file.

Error Recovery Settings

The Error Recovery Settings page enables the user to automatically reactivate a port that has been shut down because of a device error that occurs after the Automatic Recovery Interval has passed.

To configure the error recovery settings, complete these steps:

Procedure

Step 1 Click **Port Management** > **Error Recovery Settings**.

Step 2 Enter the following fields:

- Automatic Recovery Interval—Specify the time delay for automatic error recovery, if enabled, after a port is shut down.
- Automatic ErrDisable Recovery

- Port Security—Select to enable automatic error recovery when the port is shut down for port security violations.
- 802.1x Single Host Violation—Select to enable automatic error recovery when the port is shut down by 802.1x.
- ACL Deny—Select to enable automatic error recovery mechanism by an ACL action.
- STP BPDU Guard—Select to enable automatic error recovery mechanism when the port is shut down by STP BPDU guard.
- STP Loopback Guard—Enable automatic recovery when the port is shut down by STP Loopback Guard.
- UDLD—Select to enable automatic error recovery mechanism for the UDLD shutdown state.
- Loopback Detection—Select to enable error recovery mechanism for ports shut down by loopback detection.
- Storm Control—Select to enable error recovery mechanism for ports shut down by storm control.
- Link Flap Prevention—Select to enable error recovery mechanism for ports shut down by link flap prevention.

Step 3 Click **Apply** to update the global setting.

To manually reactivate a port:

Step 4 Click **Port Management** > **Error Recovery Settings**.

The list of inactivated interfaces along with their Suspension Reason is displayed.

Step 5 To filter the Suspension Reason, select a reason and click **Go**. Then, only the interfaces that are suspended for that reason are displayed in the table.

Step 6 Select the interface to be reactivated.

Step 7 Click **Reactivate**.

Loopback Detection Settings

Loopback Detection (LBD) provides protection against loops by transmitting loop protocol packets out of ports on which loop protection has been enabled. When the switch sends out a loop protocol packet, and then receives the same packet, it shuts down the port that received the packet.

Loopback Detection operates independently of STP. After a loop is discovered, the port that received the loops is placed in the Shut Down state. A trap is sent and the event is logged. Network managers can define a Detection Interval that sets the time interval between LBD packets.

To enable and configure LBD, follow these steps:

Procedure

Step 1 Click **Port Management** > **Loopback Detection Settings**.

Step 2 Select **Enable** in the Loopback Detection to enable the feature.

Step 3 Enter the Detection Interval. This is the interval between transmission of LBD packets.

Step 4 Click **Apply** to save the configuration to the Running Configuration file.

The following fields are displayed for each interface, regarding the Loopback Detection State:

- Administrative—Loopback detection is enabled.
- Operational—Loopback detection is enabled but not active on the interface.

Step 5 Select whether to enable LBD on ports or LAGS in the Interface Type equals field in the filter.

Step 6 Select the ports or LAGs on which LBD is to be enabled and click **Edit**.

Step 7 Select the settings for the chosen Interface. Next, check **Enable** in the Loopback Detection State field for the port or LAG selected.

Step 8 Click **Apply** to save the configuration to the Running Configuration file.

Link Aggregation

Link aggregation applies to various methods of combining multiple network connections in parallel in order to increase throughput beyond what a single connection could sustain. It provides redundancy in case one of the links should fail.

Link Aggregation Control Protocol (LACP) is part of the IEEE specification (802.3ad) that enables you to bundle several ports together to form a single logical channel (LAG). LAGs multiply bandwidth, increase port flexibility, and provide link redundancy between two devices.

Two types of LAGs are supported:

- Static—The ports in the LAG are manually configured. A LAG is static if LACP is disabled on it. The group of ports assigned to a static LAG are always active members. After a LAG is manually created, the LACP option can't be added or removed, until the LAG is edited and a member is removed (which can be added back prior to applying); the LACP button then become available for editing.
- Dynamic—A LAG is dynamic if LACP is enabled on it. The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports. The nonactive candidate ports are standby ports ready to replace any failing active member ports.

This section describes how to configure LAGs.

LAG Management

Link Aggregation Control Protocol (LACP) is part of the IEEE specification (802.3ad) that enables you to bundle several ports together to form a single logical channel (LAG). LAGs multiply bandwidth, increase port flexibility, and provide link redundancy between two devices.

To select the load-balancing algorithm of the LAG, follow these steps:

Procedure

Step 1 Click **Port Management** > **Link Aggregation** > **LAG Management.**

Step 2 Select one of the following Load Balance Algorithm:

- MAC Address—Perform load balancing by source and destination MAC addresses on all packets.
- IP/MAC Address—Perform load balancing by the IP addresses on the IP packets, and by MAC addresses on non-IP packets

Step 3 Click **Apply**. The Load Balance Algorithm is saved to the Running Configuration file.

To define the member or candidate ports in a LAG.

Step 4 Select the LAG to be configured, and click **Edit.**

Step 5 Enter the values for the following fields:

- LAG—Select the LAG number.
- LAG Name—Enter the LAG name or a comment.
- LACP—Select to enable LACP on the selected LAG. This makes it a dynamic LAG. This field can only be enabled after moving a port to the LAG in the next field.
- Unit—Displays the stacking member for which LAG information is defined.
- Port List—Move the ports that are assigned to the Port List LAGs to the LAG Members. Up to eight ports per static LAG can be assigned, and 16 ports can be assigned to a dynamic LAG.

Step 6 Click **Apply**. LAG membership is saved to the Running Configuration file.

LAG Settings

The LAG Settings page displays a table of current settings for all LAGs. You can configure the settings of selected LAGs, and reactivate suspended LAGs by launching the Edit LAG Settings page.

To configure the LAG settings or reactivate a suspended LAG:

Procedure

Step 1 Click **Port Management** > **Link Aggregation** > **LAG Settings**.

The LAGs in the system are displayed.

Step 2 Select a LAG, and click **Edit**.

Step 3 Enter the values for the following fields:

Option	Description
LAG	Select the LAG ID number.
LAG Type	Displays the port type that comprises the LAG.
Description	Enter the LAG name or a comment.
Administrative Status	Set the selected LAG to be Up or Down.

Option	Description
Link Status SNMP Traps	Select to enable generation of SNMP traps notifying of changes to the link status of the ports in the LAG.
Time Range	Select to enable the time range during which the port is in Up state. When the time range is not active, the port is in shutdown. If a time range is configured, it is effective only when the port is administratively up.
Time Range Name	Select the profile that specifies the time range. If a time range is not yet defined, click **Edit** to configure the time range.
Operational Status	Displays whether the LAG is currently operating.
Operational Time Range State	Displays whether the time range is currently active or inactive.
Administrative Auto Negotiation	Enables or disable auto-negotiation on the LAG. Auto-negotiation is a protocol between two link partners that enables a LAG to advertise its transmission speed and flow control to its partner (the Flow Control default is disabled). It is recommended to keep auto-negotiation enabled on both sides of an aggregate link, or disabled on both sides, while ensuring that link speeds are identical.
Administrative Speed	Select the speed of the ports in the LAG.
Administrative Advertisement	Select the capabilities to be advertised by the LAG. The options are: • Max Capability—All LAG speeds and both duplex modes are available. • 10 Full—The LAG advertises a 10 Mbps speed and the mode is full duplex. • 100 Full—The LAG advertises a 100 Mbps speed and the mode is full duplex. • 1000 Full—The LAG advertises a 1000 Mbps speed and the mode is full duplex.
Administrative Flow Control	Set Flow Control to either Enable or Disable or enable the Auto-Negotiation of Flow Control on the LAG.
Operational Auto Negotiation	Displays the auto-negotiation setting.
Operational LAG Speed	Displays the current speed at which the LAG is operating.
Operational Advertisement	Displays the Administrative Advertisement status. The LAG advertises its capabilities to its neighbor LAG to start the negotiation process. The possible values are those specified in the Administrative Advertisement field.
Operational Flow Control	Displays the current Flow Control setting.
Protected LAG	Select to make the LAG a protected port for Layer 2 isolation.

Step 4 Click **Apply**. The Running Configuration file is updated.

LACP

A dynamic LAG is LACP-enabled, and LACP is run on every candidate port defined in the LAG. LACP system priority and LACP port priority are both used to determine which of the candidate ports become active member ports in a dynamic LAG configured with more than eight candidate ports.

Use the LACP page to configure the candidate ports for the LAG and to configure the LACP parameters per port. With all factors equal, when the LAG is configured with more candidate ports than the maximum number of active ports allowed (8), the device selects ports as active from the dynamic LAG on the device that has the highest priority.



Note The LACP setting is irrelevant on ports that are not members of a dynamic LAG.

To define the LACP settings, complete the following steps:

Procedure

Step 1 Click **Port Management** > **Link Aggregation** > **LACP**.

Step 2 If needed, edit the LACP System Priority and click **Apply**.

Step 3 To edit an existing port, select the port, and click **Edit.**

Step 4 In the Edit LACP Settings dialog box, enter the values for the following fields:

- Port—Select the port number to which timeout and priority values are assigned.
- LACP Port Priority—Enter the LACP priority value for the port.
- LACP Timeout—Time interval between the sending and receiving of consecutive LACP PDUs. Select the periodic transmissions of LACP PDUs, which occur at either a Long or Short transmission speed, depending upon the expressed LACP timeout preference.

Step 5 Click **Apply**. The Running Configuration file is updated.

UDLD

UDLD is a Layer 2-protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to detect unidirectional links. A unidirectional link occurs whenever traffic from a neighboring device is received by the local device, but traffic from the local device is not received by the neighbor.

The purpose of UDLD is to detect ports on which the neighbor does not receive traffic from the local device (unidirectional link) and to shut down those ports.

All connected devices must support UDLD for the protocol to successfully detect unidirectional links. If only the local device supports UDLD, it is not possible for the device to detect the status of the link. In this case, the status of the link is set to undetermined. The user can configure whether ports in the undetermined state are shut down or not.

UDLD Global Settings

The Fiber Port UDLD Default State is only applicable to fiber ports.

The Message Time field is applicable to both copper and fiber ports.

To configure UDLD globally, follow these steps:

Procedure

Step 1 Click **Port Management** > **UDLD** > **UDLD Global Settings**.

Step 2 Enter the following fields:

- Message Time—Enter the interval between sending UDLD messages. This field is relevant for both fiber and copper ports.
- Fiber Port UDLD Default State—This field is only relevant for fiber ports. The possible states are:
  - Disabled—UDLD is disabled on all ports of the device.
  - Normal—Device shuts down an interface if the link is unidirectional. If the link is undetermined, a notification is issued.
  - Aggressive—Device shuts down an interface if the link is uni-directional. If the link is bi-directional, the device shuts down after the UDLD information times out. The port state is marked as undetermined.

Step 3 Click **Apply** to save the settings to the Running Configuration file.

UDLD Interface Settings

Use the UDLD Interface Settings page to change the UDLD state for a specific port. Here the state can be set for copper or fiber ports. To copy a particular set of values to more than one port, set that value for one port and use the Copy button to copy it to the other ports.

To configure UDLD for an interface, follow these steps:

Procedure

Step 1 Click **Port Management** > **UDLD** > **UDLD Interface Settings**.

Information is displayed for all UDLD enabled ports, or a selected group of ports.

- Port—The port identifier.
- UDLD State—The possible states are:
  - Default—Port receives the value of the Fiber Port UDLD Default State.
  - Disabled—UDLD is disabled on all fiber ports of the device.

- Normal—Device shuts down an interface if it detects that the link is unidirectional. It issues a notification if the link is undetermined.
- Aggressive—Device shuts down an interface if the link is uni-directional. If the link is bi-directional, the device shuts down after the UDLD information times out. The port state is marked as undetermined.

- Bidirectional State—The possible states are:
  - Detection—The latest UDLD state of the port is in the process of being determined. Expiration time won't expire since the last determination (if there was one), or since UDLD began running on the port, so that the state isn't yet determined.
  - Bidirectional—Traffic sent by the local device is received by its neighbor, and traffic from the neighbor is received by the local device.
  - Undetermined—The state of the link between the port and its connected port can't be determined either because no UDLD message was received or the UDLD message didn't contain the local device ID in it.
  - Disabled (Default)—UDLD has been disabled on this port.
  - Shutdown—The port has been shut down because its link with the connected device is undetermined in aggressive mode.
  - Idle—The port is idle.

- Number of Neighbors—Number of connected devices detected.

Step 2 To modify the UDLD state for a specific port, select it and click **Edit**.

Step 3 Modify the value of the UDLD state.

Step 4 Click **Apply** to save the settings to the Running Configuration file.

UDLD Neighbors

To view all devices connected to the local device, click **Port Management** > **UDLD** > **UDLD Neighbors**.

The following fields are displayed for all UDLD-enabled ports.

- Interface Name—Name of the local UDLD-enabled port.
- Neighbor Information:
  - Device ID—ID of the remote device.
  - Device MAC—MAC address of the remote device.
  - Device Name—Name of the remote device.
  - Port ID—Name of the remote port.
- State—State of the link between the local and neighboring device on the local port. The following values are possible:

- Detection—The latest UDLD state of the port is in the process of being determined. Expiration time has not yet expired since the last determination (if there was one), or since UDLD began running on the port, so that the state is not yet determined.
- Bidirectional—Traffic sent by the local device is received by its neighbor, and traffic from the neighbor is received by the local device.
- Undetermined—The state of the link between the port and its connected port cannot be determined either because no UDLD message was received or the UDLD message did not contain the local device ID in it.
- Disabled—UDLD has been disabled on this port.
- Shutdown—The port has been shut down because its link with the connected device is undetermined in aggressive mode.

- Neighbor Expiration Time (Sec.)—Displays the time that must pass before the device attempts to determine the port UDLD status. This is three times the Message Time.
- Neighbor Message Time (Sec.)—Displays the time between UDLD messages.

PoE

A PoE device is Power Sourcing Equipment (PSE) that delivers electrical power to a connected Pod Devices (PD) over existing copper cables without interfering with the network traffic, updating the physical network or modifying the network infrastructure.

PoE provides the following features:

- Eliminates the need to run 110/220 V AC power to all devices on a wired LAN.
- Eliminates the need to deploy double cabling systems in an enterprise significantly decreasing installation costs. Power over Ethernet can be used in any enterprise network that deploys relatively low-pod devices connected to the Ethernet LAN, such as: IP phones, Wireless access points, IP gateways, Audio and video remote monitoring devices.

PoE implements in the following stages:

- Detection—Sends special pulses on the copper cable. When a PoE device is located at the other end, that device responds to these pulses.
- Classification—Negotiation between the Power Sourcing Equipment (PSE) and the Pod Device (PD) commences after the Detection stage. During negotiation, the PD specifies its class, which indicates maximum amount of power that the PD consumes.
- Power Consumption—After the classification stage completes, the PSE provides power to the PD. If the PD supports PoE, but without classification, it is assumed to be class 0 (the maximum). If a PD tries to consume more power than permitted by the standard, the PSE stops supplying power to the port. PoE supports two modes:
  - Port Limit—The maximum power the device agrees to supply is limited to the value the system administrator configures, regardless of the Classification result.
  - Class Power Limit—The maximum power the device agrees to supply is determined by the results of the Classification stage. This means that it is set as per the Client's request.

Warning The PoE unit is to be connected only to PoE networks without routing to the outside plant.

Properties

Note This section is only relevant for devices supporting PoE.

The PoE Properties page enables selecting either the Port Limit or Class Limit PoE mode and specifying the PoE traps to be generated. These settings are entered in advance. When the PD actually connects and is consuming power, it might consume much less than the maximum power allowed. Output power is disabled during power-on reboot, initialization, and system configuration to ensure that PDs aren't damaged.

To configure PoE on the device and monitor current power usage:

Procedure

Step 1 Click **Port Management** > **PoE** > **Properties**.

Step 2 Enter the values for the following fields:

- Power Mode—Select one of the following options:
  - Class Limit—Maximum power limit per port is determined by the class of the device, which results from the Classification stage.
  - Port Limit—Maximum power limit per each port is configured by the user.

    Note
    When you change from Port Limit to Class Limit or conversely, disable the PoE ports, and enable them after changing the power configuration.

- Traps—Enable or disable traps. If traps are enabled, you must also enable SNMP and configure at least one SNMP Notification Recipient.
- Power Trap Threshold—Enter the usage threshold that is a percentage of the power limit. An alarm is initiated if the power exceeds this value.

  The following PoE power information is displayed for the device.
  - Nominal Power—Total amount of power the device can supply to all the connected PDs.
  - Allocated Power—The amount of power that is currently allocated to the PoE ports. The allocated power is calculated by summing the power that is allocated to each of the PoE ports. If the port negotiated power allocation with PD using CDP or LLDP then the port power allocation is based on the results of the CDP or LLDP negotiation. If the port did not negotiate the power using CDP or LLDP then the power allocated to the port equals the PD consumed power.
  - Available Power—Nominal power minus the amount of consumed power.

    Note

- Power allocation based on LLDP negotiation may be higher than the negotiated power value.
- Power allocation based on CDP negotiation will be equal to the negotiated power value.
- The power allocated per port (if different from the consumed power value) is indicated in parentheses in the “Power” column (PoE Setting Table).

- Software Version—Displays the software version of the PoE chip.
- PSE Chipset & Hardware Revision—PoE chipset and hardware revision number.

Step 3 Click **Apply** to save the PoE properties.

PoE Settings

The PoE Settings displays the system information for enabling PoE on the interfaces. It monitors the power usage and maximum power limit per port when the PoE mode is Port Limit. When the power consumed on the port exceeds the port limit, the port power is turned off.

To configure PoE settings, follow these steps:

Procedure

Step 1 Click **Port Management** > **PoE** > **PoE Settings** .

Step 2 Select a port and click **Edit**.

Step 3 Enter the value for the following field:

- Interface—Select the port to configure.
- Administrative Status—Enable or disable PoE on the port.
- Time Range—Select to enable.
- Time Range Name—If Time Range has been enabled, select the time range to be used. Click **Edit** to go to the Time Range page.
- Priority Level—Select the port priority: low, high, or critical, for use when the power supply is low. For example, if the power supply is running at 99% usage and port 1 is prioritized as high, but port 3 is prioritized as low, port 1 receives power and port 3 might be denied power.
- Administrative Power Allocation- The range depends on the port type. Ports supporting 60W PoE has a maximum value of 60000. Otherwise, maximum value is 30000. Enter a value. (Range 0- 60000, Default: 30000).
- Force Four Pair—Enable this feature to provide enhanced power supply.
- Class—Displays the class of the device, which indicates the maximum power level of the device.
- Max Power Allocation—This field appears only if the Power Mode set in the PoE Properties page is Power Limit. Displays the maximum amount of power permitted on this port.
- Negotiated Power—Power allocated to device.

Note
The "expired" warning may appear alongside the Watt value when power is allocated to the device via CDP or LLDP negotiation. When the switch stops receiving negotiation packets from the powered device, the port enters the expired state. If this happens, the port will supply power based on the most recent negotiation packet received from this device. If the device resends the negotiation packet, the port will exit the expired state and apply power based on the information in the new packet.

- Power Negotiation Protocol—Protocol determining the negotiated power.
- Power Consumption—Displays the amount of power in milliwatts assigned Settings (Class Limit)

Step 4 Click **Apply**. The PoE settings for the port are written to the Running Configuration file.

PoE Settings-Class Limits

The PoE Settings (Class Limit) Settings page displays system PoE information for enabling PoE on the interfaces and monitoring the current power usage and maximum power limit per port.

Note PoE can be configured on the device for a specific period. This feature enables you to define, per port, the days in the week and the hours that PoE is enabled. When the time range is not active, PoE is disabled.

This page limits the power per port based on the class of the connected PD. For these settings to be active, the system must be in PoE Class Limit mode. That mode is configured in the PoE Properties, on page 131. When the power consumed on the port exceeds the class limit, the port power is turned off.

To configure PoE class limit setting, complete the following steps:

Procedure

Step 1 Click **Port Management > PoE > Settings (Class Limit)**.

Ports are displayed with relevant PoE information. These fields are described in the Edit page except for the following fields:

- PoE Standard—Displays the type of PoE supported, such as 60W PoE and 802.3 AT PoE).
- Operational Status—Displays whether PoE is currently active on the port.

Step 2 Select a port and click **Edit**.

Step 3 Enter the value for the following field:

- Interface—Select the port to configure.
- Administrative Status—Check to enable.
- Time Range—Select to enabled PoE on the port.
- Time Range Name—If Time Range has been enabled, select the time range to be used. Click **Edit** to go to the Time Range page.

- Priority Level—Select the port priority: low, high, or critical, for use when the power supply is low. For example, if the power supply is running at 99% usage and port 1 is prioritized as high, but port 3 is prioritized as low, port 1 receives power and port 3 might be denied power.
- Class—Displays the class of the device, which indicates the maximum power level of the device:

Class	Maximum Power Delivered by Device Port
0	15.4 watt or 30.0 watt
1	4.0 watt
2	7.0 watt
3	15.4 watt
4	30.0 watt

- Max Power Allocation—This field appears only if the Power Mode set in the PoE Properties page is Power Limit. Displays the maximum amount of power permitted on this port.
- Negotiated Power—Power allocated to device.
- Power Negotiation Protocol—Protocol determining the negotiated power
- Power Consumption—Displays the amount of power in milliwatts assigned Settings (Class Limit)

Step 4 Click **Apply**. The PoE settings for the port are written to the Running Configuration file.

PoE Statistics

PoE consumption readings are taken every 1 minute. The daily, weekly, and monthly statistics are saved in flash memory, so that they are still available after reboot. A sample's average PoE consumption per port/device is as follows: Sum of all PoE consumption readings in a period / Number of minutes in the sampling period.

To view the PoE consumption trend on the device and define settings for the view, follow these steps:

Procedure

Step 1 Click **Port Management** > **PoE Statistics**.

Step 2 Select the port.

Step 3 Select the Refresh Rate.

Step 4 The following fields are displayed for the selected interface:

Consumption History

- Average Consumption over Last Hour—Average of all PoE consumption readings in the last hour.
- Average Consumption over Last Day—Average of all PoE consumption readings in the last day.
- Average Consumption over Last Week—Average of all PoE consumption readings in the last week.

PoE Event Counters

- Overload Counter—Number of overload conditions detected.
- Short Counter—Number of short conditions detected
- Denied Counter—Number of denied conditions detected
- Absent Counter—Number of absent conditions detected
- Invalid Signature Counter—Number of invalid signature conditions detected

Step 5 Click **View All Interfaces Statistics** to complete the following tasks:

- Clear Event Counters—Clear the displayed event counters.
- View Interface Statistics—Display the above statistics for a selected interface
- View Interface History Graph—Display the counters in graph format for a selected interface
- Refresh—Refresh the displayed counters.

Step 6 Click **View Interface History Graph**, to complete the following tasks:

- View Interface Statistics—Display the graph statistics for a selected interface in table form. Enter the Time Span in hours, days, weeks, or years.
- View All Interfaces Statistics—Display the above statistics for all interfaces in table format. Enter the Time Span in hours, days, weeks, or years.

Green Ethernet

Green Ethernet is a common name for a set of features that is designed to be environmentally friendly, and to reduce the power consumption of a device. Green Ethernet is different from EEE in that Green Ethernet energy-detect is enabled on all devices whereas only Gigabyte ports are enabled with EEE.

The Green Ethernet feature can reduce overall power usage in the following ways:

- Energy-Detect Mode—On an inactive link, the port moves into inactive mode, saving power while keeping the administrative status of the port Up. Recovery from this mode to full operational mode is fast, transparent, and no frames are lost. This mode is supported on both GE and FE ports. This mode is disabled by default.
- Short-Reach Mode—This feature provides for power savings on a short length of cable. After cable length is analyzed, the power usage is adjusted for various cable lengths. If the cable is shorter than 30 meter for 10 gigabit ports and 50 meter for other type of ports, the device uses less power to send frames over the cable, thus saving energy. This mode is only supported on RJ45 ports; it does not apply to Combo ports. This mode is disabled by default.

In addition to the above Green Ethernet features, the 802.3az Energy Efficient Ethernet (EEE) is found on devices supporting GE ports. EEE reduces power consumption when there is no traffic on the port. EEE is enabled globally by default.

Power savings, current power consumption and cumulative energy saved can be monitored. The total amount of saved energy can be viewed as a percentage of the power that would have been consumed by the physical interfaces had they not been running in Green Ethernet mode. The saved energy displayed is only related to Green Ethernet. The amount of energy saved by EEE is not displayed.

Properties

The Properties page displays and enables configuration of the Green Ethernet mode for the device. It also displays the current power savings.

To enable Green Ethernet and EEE and view power savings, follow these steps:

Procedure

Step 1 Click **Port Management** > **Green Ethernet** > **Properties**.

Step 2 Enter the values for the following fields:

- Energy Detect Mode—Click the checkbox to enable this mode. This setting isn't supported for some of the XG devices.
- Short Reach—(For non-XG devices) Click the checkbox to enable this feature.
- Port LEDs—Select to enable the port LEDs. When these are disabled, they don't display link status, activity, etc.
- 802.3 Energy Efficient Ethernet (EEE)—Globally enable or disable EEE mode. 802.3az EEE is designed to save power when there is no traffic on the link. In Green Ethernet, power is reduced when the port is down. With 802.3az EEE, power is reduced when the port is up, but there is no traffic on it.

  Note
  On Green Ethernet interfaces, the 802.3 EEE is supported for a link speed of 100Mbps and higher. On the 10G interfaces, the 802.3 EEE is supported for a link speed of 1Gbps and higher.

Step 3 Click **Reset Energy Saving Counter**—To reset the Cumulative Energy Saved information.

Step 4 Click **Apply**. The Green Ethernet Properties are written to the Running Configuration file.

Port Settings

The Port Settings displays the current Green Ethernet and EEE modes per port, and enables configuring Green Ethernet on a port using the Edit Port Setting page. For the Green Ethernet modes to operate on a port, the corresponding modes must be activated globally in Properties, on page 136.

EEE settings are only displayed for devices that have GE ports. EEE works only when ports are set to Auto negotiation. The exception is that EEE is still functional even when Auto Negotiation is disabled, but the port is at 1GB or higher. The Short reach and Energy Detect features are always enabled on XG devices and can't be disabled. On devices with FE or GE ports these features can be enabled or disabled.

To define per port Green Ethernet settings, follow these steps:

Procedure

Step 1 Click **Port Management** > **Green Ethernet** > **Port Settings**.

The Port Settings page displays the following:

- Global Parameter Status-Displays following:
  - Energy Detect Mode-Whether this mode is enabled or not.
  - Short Reach Mode-Whether this mode is enabled.
  - 802.3 Energy Efficient Ethernet (EEE) Mode-Whether this mode is enabled.

  For each port the following fields are described:

Step 2 Select a Port and click **Edit**.

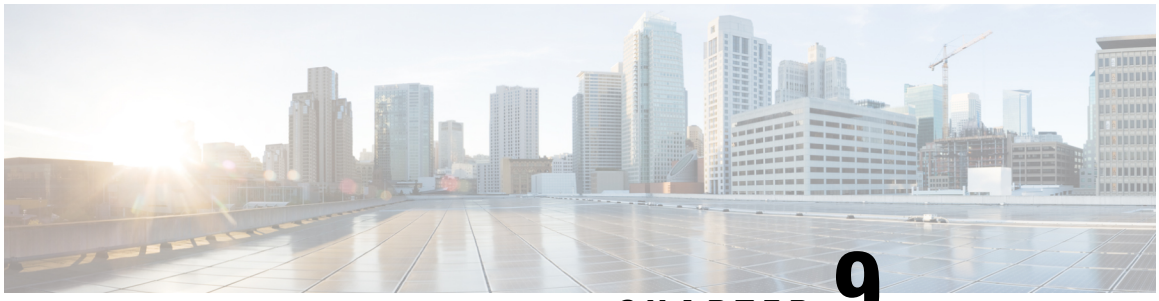
Step 3 (For non-XG devices only) Select to enable or disable Energy Detect mode on the port.

Step 4 (For non-XG devices only) Select to enable or disable Short Reach mode on the port if there are GE ports on the device.

Step 5 Select to enable or disable 802.3 Energy Efficient Ethernet (EEE) mode on the port.

Step 6 Select to enable or disable 802.3 Energy Efficient Ethernet (EEE) LLDP mode on the port (advertisement of EEE capabilities through LLDP).

Step 7 Click **Apply**. The Green Ethernet port settings are written to the Running Configuration file.



CHAPTER 9

Smartport

This chapter contains the following sections:

- Smartport Properties, on page 139
- Smartport Type Settings, on page 140
- Smartport Interface Settings, on page 141

Smartport Properties

A Smartport is an interface (port, VLAN or LAG) to which a built-in (or user-defined) macro may be applied. This Smartport feature applies a preconfigured setup to a switch port based on the type of device that is trying to connect. Auto Smartport lets the switch apply these configurations to interfaces automatically when it detects the device. Smartport types refers to the types of devices, which can be attached to Smartports.

Note If you have a 3.0.0.69 (or earlier) firmware version and you upgrade to the latest (March 2021) 3.1 version (or later when available), the default setting will remain with the Smartport feature enabled.

If you purchase a switch that has the 3.1 firmware version (or later), the firmware will have the Smartport feature **disabled** by default. This change was made because some customers didn't necessarily want to use the Smartport feature or it was causing an issue with connectivity and customers didn't realize it was enabled.

To configure the Smartport feature, follow these steps:

Procedure

Step 1 Click **Smartport** > **Properties**.

Step 2 Enter the parameters.

- Administrative Auto Smartport-Select to enable or disable Auto Smartport. The following options are available:
  - Disable-Select to disable Auto Smartport on the device. this is the default setting.
  - Enable-Select to enable Auto Smartport on the device.
  - Enable by Auto Voice VLAN-This enables the Auto Smartport, but is enabled only when Auto Voice VLAN is on.

- Operational Auto Smartport-Displays the Auto Smartport status.
- Auto Smartport Device Detection Method-Select whether incoming CDP, LLDP, or both types of packets are used to detect the Smartport type of the attaching devices. At least one must be checked for Auto Smartport to identify devices.
- Operational CDP Status-Displays the operational status of CDP. Enable CDP if Auto Smartport is to detect the Smartport type based on CDP advertisement.
- Operational LLDP Status-Displays the operational status of LLDP. Enable LLDP if Auto Smartport is to detect the Smartport type based on LLDP/LLDP-MED advertisement.
- Auto Smartport Device Detection-Select each type of device for which Auto Smartport can assign Smartport types to interfaces. If unchecked, Auto Smartport doesn't assign that Smartport type to any interface.

Step 3 Click **Apply**. This sets the global Smartport parameters on the device.

Smartport Type Settings

Use the Smartport Type Settings page to edit the Smartport Type settings and view the Macro Source. Editing the Smartport types parameters that are applied by the Auto Smartport configures the default values for these parameters.

Note Changes to Auto Smartport types cause the new settings to be applied to interfaces assigned to that type by the Auto Smartport. In this case, binding an invalid macro or setting an invalid default parameter value causes all ports of this Smartport type to become unknown.

Procedure

Step 1 Click **Smartport** > **Smartport Type Settings**.

Step 2 To view the Smartport macro associated with a Smartport type, select a Smartport type and click **View Macro Source...**.

Step 3 To modify the parameters of a macro, select a Smartport type and click **Edit**.

Step 4 Enter the fields.

- Port Type—Select a Smartport type.
- Macro Name—Displays the name of the Smartport macro currently associated with the Smartport type.
- Macro Type—Select whether the pair of macro and antimacro associated with this Smartport type is a Built-in Macro or a User-Defined Macro
- User Defined Macro—If desired, select the user-defined macro that is associated with the Smartport type. Pairing of two macros is done by name and is described in the Smartport Macro section.
- Macro Parameters—Displays the following fields for three parameters in the macro:
  - Parameter Name—Name of parameter in macro

- Parameter Value—Current value of parameter in macro
- Parameter Description—Description of parameter

Step 5 Click **Apply** to save the changes to the running configuration. If the Smartport macro and/or its parameter values associated with the Smartport type are modified, Auto Smartport automatically reapplies the macro to the interfaces currently assigned with the Smartport type by Auto Smartport. Auto Smartport does not apply the changes to interfaces that statically assigned a Smartport type.

Click **Restore Defaults** to restore the default values for the selected Smartport type.



Note There's no method to validate macro parameters because they don't have a type association. Therefore, any entry is valid at this point. However, invalid parameters can cause errors to the Smartport type assigned to an interface, applying the associated macro.

Smartport Interface Settings

Use the Interface Settings page to perform the following tasks:

- Statically apply a specific Smartport type to an interface with interface-specific values for the macro parameters.
- Enable Auto Smartport on an interface.
- Diagnose a Smartport macro that failed upon application, and caused the Smartport type to become Unknown.
- Reapply a Smartport macro to an interface. In some circumstances, you may want to reapply a Smartport macro so that the configuration at an interface is up to date. For instance, reapplying a switch Smartport macro at a device interface makes the interface a member of the VLANs created since the last macro application.
- Reset unknown interfaces, to set them to Default.

To apply a Smartport macro, follow these steps:

Procedure

Step 1 Click **Smartport** > **Interface Settings**.

To reapply the Smartport macros associated with a group of interfaces, select from the following and click **Apply**:

- All Switches, Routers, and Wireless Access Points—Reapplies the macros to all interfaces.
- All Switches—Reapplies the macros to all interfaces defined as switches.
- All Routers—Reapplies the macros to all interfaces defined as routers.

- All Wireless Access Points—Reapplies the macros to all interfaces defined as access points.

  To reapply the Smartport macros associated with an interface, select the interface and click **Reapply**.

  The Reapply action also adds the interface to all newly created VLANs.

Step 2 Smartport Diagnostic.

If a Smartport macro fails, the Smartport Type of the interface is Unknown. Select an interface which is of unknown type and click **Show Diagnostic.** This displays the command at which application of the macro failed.

Step 3 Resetting all Unknown interfaces to Default type.

- Select the Smartport Type equals to checkbox.
- Select Unknown.
- Click **Go**.
- Click **Reset All Unknown Smartports**. Then reapply the macro as described above. This performs a reset on all interfaces with type Unknown, meaning that all interfaces are returned to the Default type.

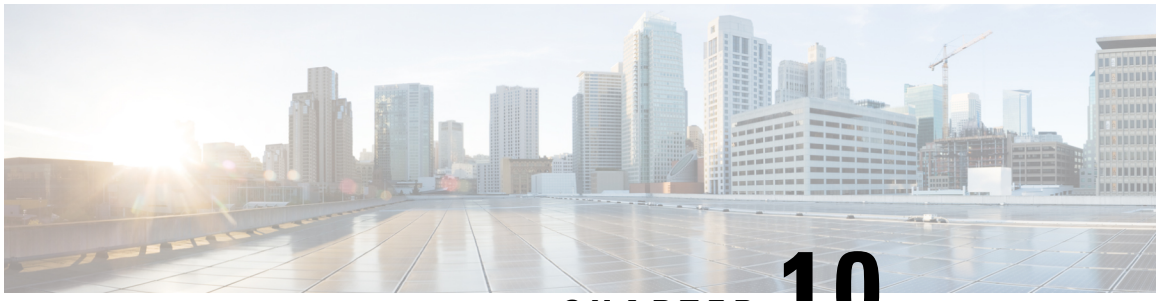
Step 4 Select an interface and click **Edit**.

Step 5 Enter the fields.

- Interface—Select the port or LAG.
- Smartport Type—Displays the Smartport type currently assigned to the port/LAG.
- Smartport Application—Select the Smartport type from the Smartport Application pull-down.
- Smartport Application Method—If Auto Smartport is selected, Auto Smartport automatically assigns the Smartport type based on the CDP and/or LLDP advertisement received from the connecting devices and applying the corresponding Smartport macro. To statically assign a Smartport type and apply the corresponding Smartport macro to the interface, select the desired Smartport type.
- Persistent Status—Select to enable the Persistent status. If enabled, the association of a Smartport type to an interface remains even if the interface goes down, or the device is rebooted. Persistent is applicable only if the Smartport Application of the interface is Auto Smartport. Enabling Persistent at an interface eliminates the device detection delay that otherwise occurs.
- Macro Parameters—Displays the following fields for up to three parameters in the macro:
  - Parameter Name—Name of parameter in macro
  - Parameter Value—Current value of parameter in macro This can be changed here.
  - Parameter Description—Description of parameter

Step 6 Click **Reset** to set an interface to Default if it is in Unknown status (as a result of an unsuccessful macro application). The macro can be reapplied on the main page.

Step 7 Click **Apply** to update the changes and assign the Smartport type to the interface.



CHAPTER 10

VLAN Management

This chapter contains the following sections:

- VLAN Settings, on page 143
- VLAN Interface Settings, on page 144
- Port to VLAN, on page 146
- Port VLAN Membership, on page 147
- VLAN Translation, on page 149
- Private VLAN Settings, on page 151
- GVRP Settings, on page 152
- VLAN Groups, on page 152
- Voice VLAN, on page 156
- Access Port Multicast TV VLAN, on page 161
- Customer Port Multicast TV VLAN, on page 163

VLAN Settings

Virtual Local Area Network (VLAN) creation allows you to make separate broadcast domains on a switch. The broadcast domains can associate with one another with the help of a Layer 3 device such as a router. A VLAN is mainly used to form groups among the hosts regardless of where the hosts are physically located. Thus, a VLAN improves security with the help of group formation among the hosts. When a VLAN is created, it has no effect until that VLAN is attached to at least one port either manually or dynamically. One of the most common reasons to set up a VLAN is to set up a separate VLAN for voice, and a separate VLAN for data. This directs the packets for both types of data despite using the same network.

To create a VLAN, follow these steps:

Procedure

Step 1 Click **VLAN Management** > **VLAN Settings**.

Step 2 Click **Add** to add one or more new VLANs.

The page enables the creation of either a single VLAN or a range of VLANs.

Step 3 To create a single VLAN, select the VLAN radio button, enter the VLAN ID, and optionally the VLAN Name.

Step 4 Add the following fields for the new VLANs.

- VLAN Interface State-Select to enable the VLAN.
- Link Status SNMP Traps-Select to enable link-status generation of SNMP traps.

Step 5 To add a range of VLANs, check **Range** and enter a VLAN Range (Range 2 - 4094) in the VLAN range field.

Step 6 Click **Apply** to create the VLAN(s).

VLAN Interface Settings

The VLAN Interface Settings page displays and enables configuration of VLAN-related parameters.

To configure the VLAN settings, follow these steps:

Procedure

Step 1 Click **VLAN Management** > **Interface Settings.**

Step 2 Select a Global Ethertype Tagging method for the S-VLAN tag.

- Dot1q-8100
- Dot1ad-88a8
- 9100
- 9200

Step 3 Select an interface type (Port or LAG), and click **Go**. Ports or LAGs and their VLAN parameters are displayed.

Step 4 To configure a Port or LAG, select it and click **Edit.**

Step 5 Enter the values for the following fields:

Interface	Select a Port/LAG.
Switchport Mode	Select either Layer 2 or Layer 3.

Interface VLAN Mode	Select the interface mode for the VLAN. The options are: • Access—The interface is an untagged member of a single VLAN. A port configured in this mode is known as an access port. • Trunk—The interface is an untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. A port configured in this mode is known as a trunk port. • General—The interface can support all functions as defined in the IEEE 802.1q specification. The interface can be a tagged or untagged member of one or more VLANs. • Customer—Selecting this option places the interface in QinQ mode. This enables you to use your own VLAN arrangements (PVID) across the provider network. The device is in Q-in-Q mode when it has one or more customer ports. • Private VLAN—Host—Select to set the interface as either isolated or community. Then select either an isolated or community VLAN in the Secondary VLAN - Host field. • Private VLAN—Promiscuous—Select to set the interface as promiscuous. • VLAN Mapping—Tunnel—Select to set the interface as a VLAN tunnel edge port. • VLAN Mapping—One to One—Select to set the interface as to be used as a VLAN mapping one to one edge port.
Ethertype Tagging	Select an Ethertype tagging method for the S-VLAN tag (see the Global Ethertype Tagging field above).
Frame Type	(Available only in General mode) Select the type of frame that the interface can receive. Frames that aren't of the configured frame type are discarded at ingress. Possible values are: • Admit All—The interface accepts all types of frames: untagged frames, tagged frames, and priority tagged frames. • Admit Tagged Only—The interface accepts only tagged frames. • Admit Untagged Only—The interface accepts only untagged and priority frames.
Ingress Filtering	Available only in General mode) Select to enable ingress filtering. When an interface is ingress filtering enabled, the interface discards all incoming frames that are classified as VLANs of which the interface isn't a member. Ingress filtering can be disabled or enabled on general ports. It's always enabled on access ports and trunk ports.
Primary VLAN	Select the primary VLAN in the private VLAN. The primary VLAN is used to allow Layer 2 connectivity from promiscuous ports to isolated ports and to community ports. If None is selected if the interface isn't in private VLAN mode.
Secondary VLAN Host	Select an isolated or community VLAN for those hosts that only require a single secondary VLAN

Available Secondary VLANs to Selected Secondary VLANs	For promiscuous ports, move all secondary VLANs that are required for normal packet forwarding from the Available Secondary VLANs. Promiscuous and trunk ports can be members in multiple VLANs

Step 6 Click **Apply**.

Port to VLAN

The Port to VLAN section displays the VLAN memberships of the ports in various presentations. You can use them to add or remove memberships to or from the VLANs.

When a port is forbidden default VLAN membership, that port isn't allowed membership in any other VLAN. An internal VID of 4095 is assigned to the port.

To forward packets, the VLAN-aware devices that carry VLAN traffic along the path between end nodes must be manually configured or must dynamically learn the VLANs and their port memberships from the Generic VLAN Registration Protocol (GVRP).

Untagged port membership between two VLAN-aware devices with no intervening VLAN-aware devices, must be to the same VLAN. The PVID on the ports between the two devices must be the same if the ports are to send and receive untagged packets to and from the VLAN. Otherwise, traffic might leak from one VLAN to another.

Frames that are VLAN-tagged can pass through other network devices that are VLAN-aware or VLAN-unaware. If a destination end node is VLAN-unaware, but is to receive traffic from a VLAN, then the last VLAN-aware device, must send frames of the destination VLAN to the end node untagged.

Use the Port to VLAN page to display and configure the ports within a specific VLAN.

To map ports or LAGs to a VLAN, follow these steps:

Procedure

Step 1 Click **VLAN Management** > **Port to VLAN**.

Step 2 Select a VLAN and the interface type (Port or LAG), and click **Go** to display or to change the port characteristic with respect to the VLAN.

The port mode for each port or LAG appears with its current port mode configured from the VLAN Interface Settings, on page 144.

Each port or LAG appears with its current registration to the VLAN.

The following fields are displayed:

- VLAN Mode—Displays port type of ports in the VLAN.
- Membership Type: Select one of the following options:
  - Forbidden—The interface isn't allowed to join the VLAN even from GVRP registration. When a port isn't a member of any other VLAN, enabling this option on the port makes the port part of internal VLAN 4095 (a reserved VID).

- Excluded—The interface is currently not a member of the VLAN. This is the default for all the ports and LAGs when the VLAN is newly created.
- Tagged—The interface is a tagged member of the VLAN.
- Untagged—The interface is an untagged member of the VLAN. Frames of the VLAN are sent untagged to the interface VLAN.
- Multicast MTV VLAN—The interface used for Digital TV using Multicast IP The port joins the VLAN with a VLAN tag of Multicast TV VLAN.

- PVID—Select to set the PVID of the interface to the VID of the VLAN. PVID is a per-port setting.

Step 3 Click **Apply**. The interfaces are assigned to the VLAN, and written to the Running Configuration file.

You can continue to display and/or configure port membership of another VLAN by selecting another VLAN ID.

Port VLAN Membership

The Port VLAN Membership page displays all ports on the device along with a list of VLANs to which each port belongs. If the port-based authentication method for an interface is 802.1x and the Administrative Port Control is Auto, then:

- Until the port is authenticated, it's excluded from all VLANs, except guest and unauthenticated ones. In the VLAN to Port page, the port is marked with an upper case P.
- When the port is authenticated, it receives membership in the VLAN in which it was configured.

Note VLAN IS mode is supported. This means that port VLAN membership can be configured ahead of time for various VLAN modes. When the port is put into the specific VLAN mode, the configuration becomes active.

To assign a port to one or more VLANs, follow these steps:

Procedure

Step 1 Click **VLAN Management** > **Port VLAN Membership**.

Step 2 Select interface type (Port or LAG), and click **Go**. The following fields are displayed for all interfaces of the selected type:

- Interface—Port/LAG ID.
- Mode—Interface VLAN mode that was selected in the VLAN Interface Settings, on page 144.
- Administrative VLANs—Drop-down list that displays all VLANs of which the interface might be a member.
- Operational VLANs—Drop-down list that displays all VLANs of which the interface is currently a member.
- LAG—If interface selected is Port, displays the LAG in which it's a member.

Step 3 Select a port, and click **Join VLAN**.

Step 4 Enter the values for the following fields:

- Interface—Select a Port or LAG.
- Current VLAN Mode—Displays the port VLAN mode that was selected in the VLAN Interface Settings, on page 144.
- Access Mode Membership (Active)
  - Access VLAN ID—Select the VLAN from the drop-down list.
  - Multicast TV VLAN—Select the multicast TV VLAN from the drop-down list.
- Trunk Mode Membership
  - Native VLAN ID—When the port is in Trunk mode, it's a member of this VLAN.
  - Tagged VLANs—When the port is in Trunk mode, it's a member of these VLANs. The following options are possible:

    All VLANs—When the port is in Trunk mode, it's a member of all VLANs.

    User Defined—When the port is in Trunk mode, it's a member of the VLANs that are entered here.
- General Mode Membership
  - Untagged VLANs—When the port is in General mode, it's an untagged member of this VLAN.
  - Tagged VLANs—When the port is in General mode, it's a tagged member of these VLANs.
  - Forbidden VLANs—When the port is in General mode, the interface isn't allowed to join the VLAN even from GVRP registration. When a port isn't a member of any other VLAN, enabling this option on the port makes the port part of internal VLAN 4095 (a reserved VID).
  - General PVID—When the port is in General mode, it's a member of these VLANs.
- Customer Mode Membership
  - Customer VLAN ID—When the port is in Customer mode, it's a member of this VLAN.
  - Customer Multicast VLANs—When the port is in Customer mode, it's a member of this Multicast TV VLAN.

Step 5 Select a port and click **Details** to view the following fields:

- Administrative VLANs—Port is configured for these VLANs.
- Operational VLANs—Port is currently a member of these VLANs.

Click **Apply** (for Join VLAN). The settings are modified and written to the Running Configuration file.

VLAN Translation

VLAN Translation is sometimes referred to when the same forwarding domain includes several different VLANS. Therefore, a frame ingressing an interface with a certain VLAN ID can be forwarded to another port with another VLAN ID.

VLAN Mapping

To configure a VLAN mapping, follow these steps:

Procedure

Step 1 Click **VLAN Management** > **VLAN Translation** > **VLAN Mapping**.

A table of previously defined VLAN mappings setting is displayed.

Step 2 Select one of the following mapping types:

- One to One—Select this option to display and edit settings of the interface set to one-to-one VLAN mapping mode.
- Tunnel Mapping—Select this option to display and edit settings of the interface set to Tunnel VLAN mapping mode.

Step 3 Click **Add** and enter the following fields:

- Interface—Select the port.
- Interface VLAN Mode—Displays the current interface mode.
- Mapping Type—Select one of the following:
  - One to One—Select this option to define one-to-one VLAN mapping settings.
  - Tunnel Mapping—Select this option to define tunnel VLAN mapping settings.
- One to One Translation—This option is available if you selected the one-to-one option in Mapping Type selection. Select one of the following:
  - Source VLAN—Configure the ID of the customer VLAN (C-VLAN) that will be translated to S-VLAN (translated VLAN).
  - Translated VLAN—Configure the S-VLAN that replaces the specified C-VLAN.
- Tunnel Mapping—This option is available if you selected the Tunnel Mapping option in the Mapping Type selection. Select one of the following:
  - Customer VLAN—Select **Default** to define the required action for C-VLANs not specified or VLAN List to specifically define VLAN tunnel behavior for listed VLANs.
  - Tunneling—Select **Drop** or Outer VLAN ID If Outer VLAN ID is selected, enter the VLANs.

Step 4 Click **Apply**. The parameters are written to the Running Configuration file.

Protocol Handling

Note In order to configure per-interface protocol handling behavior, Hardware Resources, on page 91 must be allocated to the VLAN Mapping feature.

To configure the handling of L2CP PDUs received on a VLAN translation tunnel edge port, follow these steps:

Procedure

Step 1 Click **VLAN Management** > **VLAN Translation** > **Protocol Handling**.

Note
In order to configure per-interface protocol handling behavior, hardware resources must be allocated to the VLAN Mapping feature.

Step 2 Optionally, set the Default Tunneling CoS: enter a value between 0-7 (default=5) to define a global CoS value to apply to L2CP PDUs which are forwarded and encapsulated on VLAN tunneling edge ports. This value is used for all interfaces that do not have specific user CoS settings.

Step 3 Select one of the entries listed and click **Copy Settings** to copy the settings in the selected entry to one or more entries. Click **Edit** to edit the selected entry.

Step 4 Enter the following fields.

- Interface—Select the port.
- Interface VLAN Mode—Displays the current interface VLAN mode
- BPDU VLAN ID—Select one of the following:
  - None—there is no VLAN selected for L2CP BPDU tunneling. Use this selection to disable tunneling L2CP PDUs.
  - vlan-id—one of the VLAN IDs configured on device - select one of the available VLAN IDs to use for tunneling L2CP PDUs on this interface.
- CoS—Select one of the following:
  - Use Default—Select this to use the global default value
  - User Defined—Select this option set a value between 0-7.
- Drop Threshold—Select one of the following:
  - None—Select this to disable the drop threshold.

- User Defined—Select this option to set the drop threshold. Valid values are between 8-256 Kbps (default is 32Kbps).

- Protocol Forwarding—Check the protocols that the device will forward and encapsulate:
  - CDP —Check to enable forwarding and encapsulating this protocol.
  - LLDP —Check to enable forwarding and encapsulating this protocol
  - STP —Check to enable forwarding and encapsulating this protocol.
  - VTP —Check to enable forwarding and encapsulating this protocol.

Step 5 Click **Apply**. The parameters are written to the Running Configuration file.

Private VLAN Settings

The Private VLAN feature provides layer-2 isolation between ports. This means that at the level of bridging traffic, as opposed to IP routing, ports that share the same Broadcast domain cannot communicate with each other. The ports in a private VLAN can be located anywhere in the layer 2 network, meaning that they do not have to be on the same switch. The private VLAN is designed to receive untagged or priority-tagged traffic and transmit untagged traffic.

Note Interface membership in the Private VLANs is configured on the VLAN Interface Settings, on page 144. Use Private VLAN—Host interface mode for Community and Isolated VLANs, or Private VLAN—Promiscuous interface mode for Primary VLAN.

To create a new private VLAN, follow these steps:

Procedure

Step 1 Click **VLAN Management** > **Private VLAN Settings**.

Step 2 Click **Add**.

Step 3 Enter the values for the following fields:

- Primary VLAN ID—Select a VLAN to be defined as the primary VLAN in the private VLAN. The primary VLAN is used to allow Layer 2 connectivity from promiscuous ports to isolated ports and to community ports.
- Isolated VLAN ID—An isolated VLAN is used to allow isolated ports to send traffic to the primary VLAN.
- Available Community VLANs—Move the VLANs that you want to be community VLANs to the Selected Community VLANs list. Community VLANs allow Layer 2 connectivity from community ports to promiscuous ports and to community ports of the same community. This is called Community VLAN Range on the main page.

Step 4 Click **Apply**. The settings are modified and written to the Running Configuration file.

GVRP Settings

Adjacent VLAN-aware devices can exchange VLAN information with each other by using the Generic VLAN Registration Protocol (GVRP). GVRP is based on the Generic Attribute Registration Protocol (GARP) and propagates VLAN information throughout a bridged network.

GVRP must be activated globally and on each port. When it's activated, it transmits and receives GARP Packet Data Units (GPDUs). VLANs that are defined but not active aren't propagated. To propagate the VLAN, it must be up on at least one port. By default, GVRP is disabled globally and on ports.

To define GVRP settings for an interface:

Procedure

Step 1 Click **VLAN Management** > **GVRP Settings**.

Step 2 Select **GVRP Global Status** to enable GVRP globally.

Step 3 Click **Apply** to set the global GVRP status.

Step 4 Select an interface type (Port or LAG), and click **Go** to display all interfaces of that type.

Step 5 To define GVRP settings for a port, select it, and click **Edit.**

Step 6 Enter the values for the following fields:

- Interface—Select the interface (Port or LAG) to be edited.
- GVRP State—Select to enable GVRP on this interface.
- Dynamic VLAN Creation—Select to enable Dynamic VLAN Creation on this interface.
- GVRP Registration—Select to enable VLAN Registration using GVRP on this interface.

Step 7 Click **Apply**. GVRP settings are modified, and written to the Running Configuration file.

VLAN Groups

VLAN groups are used for load balancing of traffic on a Layer 2 network. Packets are assigned a VLAN according to various classifications.

If several classifications schemes are defined, packets are assigned to a VLAN in the following order:

- TAG—If the packet is tagged, the VLAN is taken from the tag.
- MAC-Based VLAN—If a MAC-based VLAN has been defined, the VLAN is taken from the source MAC-to-VLAN mapping of the ingress interface.

- Subnet-Based VLAN—If a subnet-based VLAN has been defined, the VLAN is taken from the source IP-to-VLAN mapping of the ingress interface.
- Protocol-Based VLAN—If a protocol-based VLAN has been defined, the VLAN is taken from the (Ethernet type) protocol-to-VLAN mapping of the ingress interface.
- PVID—VLAN is taken from the port default VLAN ID.

MAC-Based Groups

MAC-based VLAN classifications enable packets to be classified by their source MAC address. You can then define MAC-to-VLAN mapping per interface. You can define several MAC-based VLAN groups, which each group containing different MAC addresses. These MAC-based groups can be assigned to specific ports/LAGs. MAC-based VLAN groups can't contain overlapping ranges of MAC addresses on the same port.

To assign a MAC address to a VLAN Group, complete the following steps:

Procedure

Step 1 Click **VLAN Management** > **VLAN Groups** > **MAC-Based Groups**.

Step 2 Click **Add.**

Step 3 Enter the values for the following fields:

- MAC Address—Enter a MAC address to be assigned to a VLAN group.

  Note
  This MAC address can't be assigned to any other VLAN group.

- Prefix Mask—Enter one of the following:
  - Host(48)—To include all bits of MAC address in the prefix mask (48 bits)
  - Length—Prefix of the MAC address
- Group ID—Enter a user-created VLAN group ID number.

Step 4 Click **Apply**. The MAC address is assigned to a VLAN group.

MAC-Based Groups to VLAN

To assign a MAC-based VLAN group to a VLAN on an interface, complete the following:

Procedure

Step 1 Click **VLAN Management** > **VLAN Groups** > **MAC-Based Groups to VLAN.**

Step 2 Click **Add.**

Step 3 Enter the values for the following fields:

- Group Type—Displays that the group is MAC-Based.
- Interface—Enter a general interface (port/LAG) through which traffic is received.
- Group ID—Select a VLAN group.
- VLAN ID—Select the VLAN to which traffic from the VLAN group is forwarded.

Step 4 Click **Apply** to set the mapping of the VLAN group to the VLAN. This mapping does not bind the interface dynamically to the VLAN; the interface must be manually added to the VLAN.)

Subnet-Based Groups

The subnet-based group VLAN classification enable packets to be classified according to their subnet. You can then define subnet-to-VLAN mapping per interface. You can define several subnet-based VLAN groups, which each group containing different subnets.

These groups can be assigned to specific ports/LAGs. Subnet-based VLAN groups cannot contain overlapping ranges of subnets on the same port.

To add a subnet-based group, complete the following steps:

Procedure

Step 1 Click **VLAN Management** > **VLAN Groups** > **Subnet-Based Groups**.

Step 2 Click **Add**.

Step 3 Enter the following fields:

- IP Address—Enter the IP address on which the subgroup is based.
- Prefix Mask—Enter the prefix mask that defines the subnet.
- Group ID—Enter a group ID.

Step 4 Click **Apply**. The group is added, and written to the Running Configuration file.

Subnet-Based Groups to VLAN

To map a subnet group to a port, the port must not have DVA configured on it (see VLAN Interface Settings, on page 144). Several groups can be bound to a single port, with each port being associated to its own VLAN. It is possible to map several groups to a single VLAN as well.

To map the subnet group to a VLAN, follow these steps:

Procedure

Step 1 Click **VLAN Management** > **VLAN Groups** > **Subnet-Based Groups to VLAN.**

Step 2 To associate an interface with a protocol-based group and VLAN, click **Add.**

The Group Type field displays the type of group being mapped.

Step 3 Enter the following fields.

- Interface—Port or LAG number assigned to VLAN according to protocol-based group.
- Group ID—Protocol group ID.
- VLAN ID—Attaches the specified group for this interface to a user-defined VLAN ID.

Step 4 Click **Apply**. The subnet-based group ports are mapped to VLANs, and written to the Running Configuration file.

Protocol-Based Groups

Groups of protocols can be defined and then bound to a port. After the protocol group is bound to a port, every packet originating from a protocol in the group is assigned the VLAN that is configured in the Protocol-Based Groups page. To define a set of protocols, follow these steps.

Procedure

Step 1 Click **VLAN Management** > **VLAN Groups** > **Protocol-Based Groups**.

Step 2 Click **Add** to add a protocol-based VLAN group.

Step 3 Enter the following fields:.

- Encapsulation—Protocol Packet type. The following options are available:
  - Ethernet V2—If this is selected, select the Ethernet Type.
  - LLC-SNAP (rfc1042)—If this is selected, enter the Protocol Value.
  - LLC—If this is selected, select the DSAP-SSAP Values.
- Ethernet Type—Select the Ethernet type for Ethernet V2 encapsulation. This is the two-octet field in the Ethernet frame used to indicate which protocol is encapsulated in the payload of the Ethernet packet) for the VLAN group.
- Protocol Value—Enter the protocol for LLC-SNAP (rfc 1042) encapsulation.
- Group ID—Enter a protocol group ID.

Step 4 Click **Apply**. The Protocol Group is added, and written to the Running Configuration file.

Protocol-Based Groups to VLAN

Protocol-based VLANs divide the physical network into logical VLAN groups for each protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type. Several groups can be bound to a single port, with each port being associated to its own VLAN. It's possible to map several groups to a single VLAN as well.

To map the protocol port to a VLAN, follow these steps:

Procedure

Step 1 Click **VLAN Management** > **VLAN Groups** > **Protocol-Based Groups to VLAN.**

Step 2 To associate an interface with a protocol-based group and VLAN, click **Add.**

The Group Type field displays the type of group being mapped.

Step 3 Enter the following fields.

- Interface—Port or LAG number assigned to VLAN according to protocol-based group.
- Group ID—Protocol group ID.
- VLAN ID—Attaches the interface to a user-defined VLAN ID.

Step 4 Click **Apply**. The protocol ports are mapped to VLANs, and written to the Running Configuration file.

Voice VLAN

The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone. When the switch is connected to an IP Phone, the phone sends voice traffic with Layer 3 IP precedence and Layer 2 class of service (CoS) values, which are both set to 5 by default. Because the sound quality of an IP phone call can deteriorate if the data is unevenly sent, the switch supports quality of service (QoS) based on IEEE 802.1p CoS. QoS uses classification and scheduling to send network traffic from the switch in a predictable manner.

Voice VLAN can propagate the CoS/802.1p and DSCP settings by using LLDP-MED Network policies. The LLDP-MED is set by default to response with the Voice QoS setting if an appliance sends LLDP-MED packets. MED-supported devices must send their voice traffic with the same CoS/802.1p and DSCP values, as received with the LLDP-MED response.You can disable the automatic update between Voice VLAN and LLDP-MED and use your own network polic ies. Working with the OUI mode, the device can additionally configure the mapping and remarking (CoS/802.1p) of the voice traffic based on the OUI.

By default, all interfaces are CoS/802.1p trusted. The device applies the quality of service based on the CoS/802.1p value found in the voice stream. For Telephony OUI voice streams, you can override the quality of service and optionally remark the 802.1p of the voice streams by specifying the desired CoS/802.1p values and using the remarking option under Telephony OUI.

Properties

Use the Voice VLAN Properties page for the following:

- View how voice VLAN is currently configured.
- Configure the VLAN ID of the Voice VLAN.
- Configure voice VLAN QoS settings.
- Configure the voice VLAN mode (Telephony OUI or Auto Voice VLAN).
- Configure how Auto Voice VLAN is triggered.

To view and configure Voice VLAN properties:

Procedure

Step 1 Click **VLAN Management** > **Voice VLAN** > **Properties**.

- The voice VLAN settings configured on the device are displayed in the Voice VLAN Settings (Administrative Status) block.
- The voice VLAN settings that are actually being applied to the voice VLAN deployment are displayed in the Voice VLAN Settings (Operational Status) block.

Step 2 Enter values for the following Administrative Status fields:

- Voice VLAN ID—Enter the VLAN that is to be the Voice VLAN.

  Note
  Changes in the voice VLAN ID, CoS/802.1p, and/or DSCP cause the device to advertise the administrative voice VLAN as a static voice VLAN. If the option Auto Voice VLAN Activation triggered by external Voice VLAN is selected, then the default values need to be maintained.

- CoS/802.1p —Select a CoS/802.1p value for the LLDP-MED as a voice network policy. Refer to Administration > Discovery > LLDP > LLDP MED Network Policy for more details.
- DSCP—Selection of DSCP values for the LLDP-MED as a voice network policy. Refer to Administration > Discovery > LLDP > LLDP MED Network Policy for more details.

The following Operational Status fields are displayed:

- Voice VLAN ID—Voice VLAN.
- CoS/802.1p —Value being used by LLDP-MED as a voice network policy. Refer to Administration > Discovery > LLDP > LLDP MED Network Policy for more details.
- DSCP—Value used by the LLDP-MED as a voice network policy.

The following Dynamic Voice VLAN Settings fields are displayed:

- Dynamic Voice VLAN—Select this field to disable or enable voice VLAN feature in one of the following ways:
  - Enable Auto Voice VLAN—Enable Dynamic Voice VLAN in Auto Voice VLAN mode.
  - Enable Telephony OUI—Enable Dynamic Voice VLAN in Telephony OUI mode.
  - Disable-Disable Auto Voice VLAN or Telephony OUI

- Auto Voice VLAN Activation—If Auto Voice VLAN was enabled, select one of the following options to activate Auto Voice VLAN:
  - Immediate—Auto Voice VLAN on the device is to be activated and put into operation immediately if enabled.
  - By external Voice VLAN trigger—Auto Voice VLAN on the device is activated and put into operation only if the device detects a device advertising the voice VLAN.

  Note
  Manually reconfiguring the voice VLAN ID, CoS/802.1p, and/or DSCP from their default values results in a static voice VLAN, which has higher priority than auto voice VLAN.

Step 3 Click **Apply**. The VLAN properties are written to the Running Configuration file.

Auto Voice VLAN

If Auto Voice VLAN mode is enabled, use the Auto Voice VLAN page to view the relevant global and interface parameters.

You can also use this page to manually restart Auto Voice VLAN, by clicking Restart Auto Voice VLAN. After a short delay, this resets the voice VLAN to the default voice VLAN and restarts the Auto Voice VLAN discovery and synchronization process on all the switches in the LAN that are Auto Voice VLAN enabled.

Note This only resets the voice VLAN to the default voice vlan if the Source Type is in the Inactive state.

To view Auto Voice VLAN parameters:

Procedure

Step 1 Click **VLAN Management** > **Voice VLAN** > **Auto Voice VLAN**.

The Operational Status block on this page shows the information about the current voice VLAN and its source:

- Auto Voice VLAN Status—Displays whether Auto Voice VLAN is enabled.
- Voice VLAN ID—The identifier of the current voice VLAN
- Source Type—Displays the type of source where the voice VLAN is discovered by the root device.
- CoS/802.1p—Displays CoS/802.1p values to be used by the LLDP-MED as a voice network policy.
- DSCP—Displays DSCP values to be used by the LLDP-MED as a voice network policy.
- Root Switch MAC Address—The MAC address of the Auto Voice VLAN root device that discovers or is configured with the voice VLAN from which the voice VLAN is learned.
- Switch MAC Address—Base MAC address of the device. If the device's Switch MAC address is the Root Switch MAC Address, the device is the Auto Voice VLAN root device.
- Voice VLAN ID Change Time—Last time that voice VLAN was updated.

Step 2 Click **Restart Auto Voice VLAN** to reset the voice VLAN to the default voice VLAN and restart Auto Voice VLAN discovery on all the Auto-Voice-VLAN-enabled switches in the LAN.

The Voice VLAN Local Source Table displays voice VLAN configured on the device, and any voice VLAN configuration advertised by directly connected neighbor devices. It contains the following fields:

- Interface—Displays the interface on which voice VLAN configuration was received or configured. If N/A appears, the configuration was done on the device itself. If an interface appears, a voice configuration was received from a neighbor.
- Source MAC Address—MAC address of a UC from which the voice configuration was received.
- Source Type—Type of UC from which voice configuration was received. The following options are available:
  - Default—Default voice VLAN configuration on the device
  - Static—User-defined voice VLAN configuration defined on the device
  - CDP—UC that advertised voice VLAN configuration is running CDP.
  - LLDP—UC that advertised voice VLAN configuration is running LLDP.
  - Voice VLAN ID—The identifier of the advertised or configured voice VLAN
- Voice VLAN ID—The identifier of the current voice VLAN.
- CoS/802.1p—The advertised or configured CoS/802.1p values that are used by the LLDP-MED as a voice network policy.
- DSCP—The advertised or configured DSCP values that are used by the LLDP-MED as a voice network policy.
- Best Local Source—Displays whether this voice VLAN was used by the device. The following options are available:
  - Yes—The device uses this voice VLAN to synchronize with other Auto Voice VLAN-enabled switches. This voice VLAN is the voice VLAN for the network unless a voice VLAN from a higher priority source is discovered. Only one local source is the best local source.
  - No—This isn't the best local source.

Step 3 Click **Refresh** to refresh the information on the page

Telephony OUI

OUIs are assigned by the Institute of Electrical and Electronics Engineers, Incorporated (IEEE) Registration Authority. Since the number of IP phone manufacturers is limited and well-known, the known OUI values cause the relevant frames, and the port on which they are seen, to be automatically assigned to a Voice VLAN. Use the Telephony OUI page to configure Telephony OUI QoS properties. In addition, the Auto Membership Aging time can be configured. If the specified time period passes with no telephony activity, the port is removed from the Voice VLAN.

To configure Telephony OUI and/or add a new Voice VLAN OUI:

Procedure

Step 1 Click **VLAN Management** > **Voice VLAN** > **Telephony OUI**.

The Telephony OUI page contains the following fields:

- Telephony OUI Operational Status—Displays whether OUIs are used to identify voice traffic.
- CoS/802.1p—Select the CoS queue to be assigned to voice traffic.
- Remark CoS/802.1p—Select whether to remark egress traffic.
- Auto Membership Aging Time—Enter the time delay to remove a port from the voice VLAN after all of the MAC addresses of the phones detected on the ports have aged out.

Step 2 Click **Apply** to update the Running Configuration of the device with these values.

The Telephony OUI table appears:

- Telephony OUI—First six digits of the MAC address that are reserved for OUIs.
- Description—User-assigned OUI description.

Step 3 Click **Restore Default OUIs** to delete all of the user-created OUIs, and leave only the default OUIs in the table. The OUI information may not be accurate until the restoration is completed. This may take several seconds. After several seconds have passed, refresh the page by exiting it and reentering it.

To delete all the OUIs, select the top checkbox. All the OUIs are selected and can be deleted by clicking **Delete**. If you then click **Restore Default OUIs**, the system recovers the known OUIs.

Step 4 To add a new OUI, click **Add.**

Step 5 Enter the values for the following fields:

- Telephony OUI—Enter a new OUI.
- Description—Enter an OUI name.

Step 6 Click **Apply**. The OUI is added to the Telephony OUI Table.

Telephone OUI Interface

The QoS attributes can be assigned per port to the voice packets in one of the following modes:

- All—Quality of Service (QoS) values configured to the Voice VLAN are applied to all of the incoming frames that are received on the interface and are classified to the Voice VLAN.
- Telephony Source MAC Address (SRC)—The QoS values configured for the Voice VLAN are applied to any incoming frame that is classified to the Voice VLAN and contains an OUI in the source MAC address that matches a configured telephony OUI.

Use the Telephony OUI Interface page to add an interface to the voice VLAN on the basis of the OUI identifier and to configure the OUI QoS mode of voice VLAN.

To configure Telephony OUI on an interface:

Procedure

Step 1 Click **VLAN Management** > **Voice VLAN** > **Telephony OUI Interface**.

The Telephony OUI Interface page contains voice VLAN OUI parameters for all interfaces.

Step 2 To configure an interface to be a candidate port of the telephony OUI-based voice VLAN, click **Edit.**

Step 3 Enter the values for the following fields:

- Interface—Select an interface.
- Telephony OUI VLAN Membership—If enabled, the interface is a candidate port of the telephony OUI based voice VLAN. When packets that match one of the configured telephony OUI are received, the port is added to the voice VLAN.
- Voice VLAN QoS Mode (Telephone OUI QoS Mode in main page)—Select one of the following options:
  - All—QoS attributes are applied on all packets that are classified to the Voice VLAN.
  - Telephony Source MAC Address—QoS attributes are applied only on packets from IP phones.

Step 4 Click **Apply**. The OUI is added.

Access Port Multicast TV VLAN

Multicast TV VLANs enable Multicast transmissions to subscribers who are not on the same data VLAN (Layer 2-isolated), without replicating the Multicast transmission frames for each subscriber VLAN.

Subscribers, who are not on the same data VLAN (Layer 2-isolated) and are connected to the device with different VLAN ID membership, can share the same Multicast stream by joining the ports to the same Multicast VLAN ID.

The network port, connected to the Multicast server, is statically configured as a member in the Multicast VLAN ID.

The network ports, which through subscribers communicate with the Multicast server (by sending IGMP messages), receive the Multicast streams from the Multicast server, while including the Multicast TV VLAN in the Multicast packet header. For this reasons, the network ports must be statically configured as the following:

- Trunk or general port type (see VLAN Interface Settings, on page 144)
- Member of the Multicast TV VLAN

The subscriber receiver ports can be associated with the Multicast TV VLAN only if it is defined as an access port.

One or more IP Multicast address groups can be associated with the same Multicast TV VLAN.

Any VLAN can be configured as a Multicast-TV VLAN. A port assigned to a Multicast-TV VLAN:

- Joins the Multicast-TV VLAN.
- Packets passing through egress ports in the Multicast TV VLAN are untagged.
- The port's Frame Type parameter is set to Admit All, allowing untagged packets (see VLAN Interface Settings, on page 144).

The Multicast TV VLAN configuration is defined per port. Customer ports are configured to be member of Multicast TV VLANs using the Port Multicast VLAN Membership page.

Multicast Group to VLAN

You can map up to 256 ranges of IPv4 addresses to a Multicast TV VLAN. In each range, you can configure the full scope of Multicast addresses.



Note An * indicates that the corresponding Multicast Group is inactive because the associated Multicast TV VLAN does not exist. Go to the VLAN Settings, on page 143 to create the VLAN.

To define the Multicast TV VLAN configuration, follow these steps:

Procedure

Step 1 Click **VLAN Management** > **Access Port Multicast TV VLAN** > **Multicast Group to VLAN**.

Step 2 Click **Add** to associate a Multicast group to a VLAN. Any VLAN can be selected.

Enter the following fields:

- Multicast TV VLAN-VLAN to which the Multicast packets are assigned. When a VLAN is selected here, it becomes a Multicast TV VLAN.
- Multicast Group Start-First IPv4 address of the Multicast group range.
- Group Definition-Select one of the following range options:
  - By group size-Specify the number of Multicast addresses in the group range.
  - By range-Specify an IPv4 Multicast address greater than the address in the Multicast Group Start field. This is the last address of the range.

Step 3 Click **Apply**. Multicast TV VLAN settings are modified, and written to the Running Configuration file.

Port Multicast TV VLAN Membership

To define the Multicast TV VLAN configuration:

Procedure

Step 1 Click **VLAN Management** > **Access Port Multicast TV VLAN** > **Port Multicast VLAN Membership**.

Step 2 Select a VLAN from Multicast TV VLAN.

Step 3 Select an interface from Interface Type.

Step 4 The Candidate Access Ports list contains all access ports configured on the device. Move the required ports to the Member Access Ports field.

Step 5 Click **Apply**. Multicast TV VLAN settings are modified, and written to the Running Configuration file.

Customer Port Multicast TV VLAN

A triple play service provisions three broadband services, over a single broadband connection:

- High-speed Internet access
- Video
- Voice

The triple play service is provisioned for service provider subscribers, while keeping Layer 2-isolation between them.

Each subscriber has a CPE MUX box. The MUX has multiple access ports that are connected to the subscriber's devices (PC, telephone and so on), and one network port that is connected to the access device.

The box forwards the packets from the network port to the subscriber's devices based on the VLAN tag of the packet. Each VLAN is mapped to one of the MUX access ports.

Packets from subscribers to the service provider network are forwarded as VLAN tagged frames, in order to distinguish between the service types, which mean that for each service type there is a unique VLAN ID in the CPE box.

All packets from the subscriber to the service provider network are encapsulated by the access device with the subscriber’s VLAN configured as customer VLAN (Outer tag or S-VID), except for IGMP snooping messages from the TV receivers, which are associated with the Multicast TV VLAN. VOD information that is also sent from the TV receivers are sent like any other type of traffic.

Packets from the service provider network that received on the network port to the subscriber are sent on the service provider network as double tag packets, while the outer tag (Service Tag or S-Tag) represent one of the two type of VLAN as following:

- Subscriber’s VLAN (Includes Internet and IP Phones)
- Multicast TV VLAN

The inner VLAN (C-Tag) is the tag that determines the destination in the subscriber’s network (by the CPE MUX).

CPE VLAN to VLAN

To support the CPE MUX with subscribers VLANs, subscribers may require multiple video providers, and each provider is assigned a different external VLAN.

CPE (internal) Multicast VLANs must be mapped to the Multicast provider (external) VLANs.

After a CPE VLAN is mapped to a Multicast VLAN, it can participate in IGMP snooping.

To map CPE VLANs, follow these steps:

Procedure

Step 1 Click **VLAN Management** > **Customer Port Multicast TV VLAN** > **CPE VLAN to VLAN.**

Step 2 Click **Add**.

Step 3 Enter the following fields:

- CPE VLAN-Enter the VLAN defined on the CPE box.
- Multicast TV VLAN-Select the Multicast TV VLAN which is mapped to the CPE VLAN.

Step 4 Click **Apply**. CPE VLAN Mapping is modified, and written to the Running Configuration file.

Port Multicast VLAN Membership

The ports associated with the Multicast VLANs must be configured as customer ports (see VLAN Interface Settings, on page 144).

To map ports to Multicast TV VLANs, follow these steps, follow these steps:

Procedure

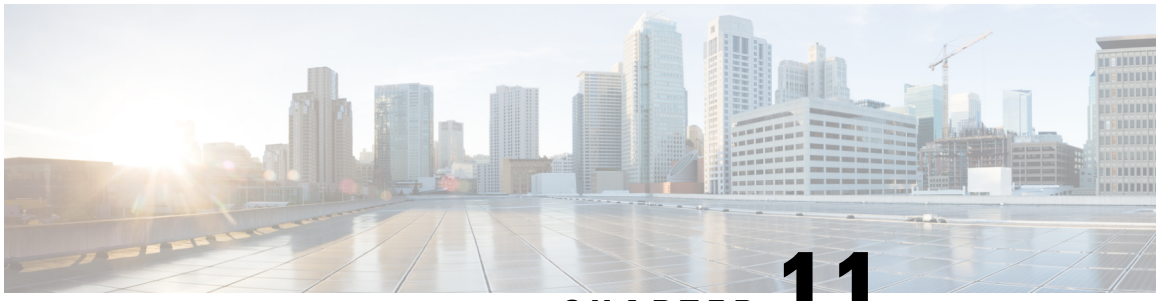
Step 1 Click **VLAN Management** > **Customer Port Multicast TV VLAN** > **Port Multicast VLAN Membership**.

Step 2 Select a VLAN from Multicast TV VLAN.

Step 3 Select an interface from Interface Type.

Step 4 The Candidate Customer Ports list contains all access ports configured on the device. Move the required ports to the Member Customer Ports field.

Step 5 Click **Apply**. The new settings are modified, and written to the Running Configuration file.



CHAPTER 11

Spanning Tree

This chapter contains the following sections:

- STP Status and Global Settings, on page 165
- STP Interface Settings, on page 166
- RSTP Interface Settings, on page 169
- MSTP, on page 170
- PVST, on page 175

STP Status and Global Settings

Spanning Tree Protocol (STP) protects a Layer 2 Broadcast domain from Broadcast storms by selectively setting links to standby mode to prevent loops. In standby mode, these links temporarily stop transferring user data. After the topology changes so that the data transfer is made possible, the links are automatically re-activated.

STP provides a tree topology for any arrangement of switches and interconnecting links, by creating a unique path between end stations on a network, and thereby eliminating loops.

The STP Status and Global Settings page contains parameters for enabling the required STP mode. Use the STP Interface Settings page, RSTP Interface Settings page, and MSTP Properties page to configure each mode, respectively. To set the STP status and global settings, follow these steps:

Procedure

Step 1 Click **Spanning Tree** > **STP Status & Global Settings**.

Step 2 Enter the parameters.

Global Settings:

Spanning Tree State	Select to enable on the device.
STP Loopback Guard	Select to enable Loopback Guard on the device.
STP Operation Mode	Select an STP mode.

BPDU Handling	Select how Bridge Protocol Data Unit (BPDU) packets are managed when STP is disabled. BPDUs are used to transmit spanning tree information. • Filtering-Filters BPDU packets when Spanning Tree is disabled on an interface. • Flooding-Floods BPDU packets when Spanning Tree is disabled on an interface.
Path Cost Default Values	Selects the method used to assign default path costs to the STP ports. The default path cost assigned to an interface varies according to the selected method. • Short-Specifies the range 1–65,535 for port path costs • Long-Specifies the range 1–200,000,000 for port path costs Bridge Settings:

Bridge Settings:

Priority	Sets the bridge priority value. After exchanging BPDUs, the device with the lowest priority becomes the Root Bridge. In the case that all bridges use the same priority, then their MAC addresses are used to determine the Root Bridge. The bridge priority value is provided in increments of 4096. For example, 4096, 8192, 12288, and so on.
Hello Time	Set the interval (in seconds) that a Root Bridge waits between configuration messages.
Max Age	Set the interval (in seconds) that the device can wait without receiving a configuration message, before attempting to redefine its own configuration.
Forward Delay	Set the interval (in seconds) that a bridge remains in a learning state before forwarding packets. For more information, refer to STP Interface Settings, on page 166.
Designated Root / Bridge ID	The bridge priority concatenated with the MAC address of the device.
Root Bridge ID	The Root Bridge priority concatenated with the MAC address of the Root Bridge.
Root Port	The port that offers the lowest cost path from this bridge to the Root Bridge.
Root Path Cost	The cost of the path from this bridge to the root.
Topology Changes Counts	The total number of STP topology changes that have occurred.
Last Topology Change	The time interval that elapsed since the last topology change occurred. The time appears in a days/hours/minutes/seconds format.

Step 3 Click **Apply**. The STP Global settings are written to the Running Configuration file.

STP Interface Settings

The STP Interface Settings page enables you to configure STP on a per-port basis, and to view the information learned by the protocol, such as the designated bridge.

The defined configuration entered is valid for all flavors of the STP protocol.

To configure STP on an interface, follow these steps:

Procedure

Step 1 Click **Spanning Tree** > **STP Interface Settings**.

Step 2 Select an interface and click **Edit**.

Step 3 Enter the parameters

Interface	Select the Port or LAG on which Spanning Tree is configured.
STP	Enables or disables STP on the port.
Edge Port	Enables or disables Fast Link on the port. If Fast Link mode is enabled on a port, the port is automatically set to Forwarding state when the port link is up. Fast Link optimizes the STP protocol convergence. The options are: • Enable—Enables Fast Link immediately • Auto—Enables Fast Link a few seconds after the interface becomes active. This allows STP to resolve loops before enabling Fast Link • Disable—Disables Fast Link **Note** It's recommended to set the value to Auto so that the device sets the port to fast link mode if a host is connected to it, or sets it as a regular STP port if connected to another device. This helps avoid loops. Edge Port isn't operational in MSTP mode.
Root Guard	Root Guard—Enables or disables Root Guard on the device. The Root Guard option provides a way to enforce the root bridge placement in the network Root Guard ensures that the port on which this feature is enabled is the designated port. Normally, all root bridge ports are designated ports, unless two or more ports of the root bridge are connected. If the bridge receives superior BPDUs on a Root Guard-enabled port, Root Guard moves this port to a root-inconsistent STP state. This root-inconsistent state is effectively equal to a listening state. No traffic is forwarded across this port. In this way, Root Guard enforces the position of the root bridge.
BPDU Guard	BPDU Guard—Enables or disables the Bridge Protocol Data Unit (BPDU) Guard feature on the port. The BPDU Guard enables you to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have BPDU Guard enabled can't influence the STP topology. At the reception of BPDUs, the BPDU guard operation disables the port that has BPDU configured. In this case, a BPDU message is received, and an appropriate SNMP trap is generated.

BPDU Handling	Select how BPDU packets are managed when STP is disabled on the port or the device. BPDUs are used to transmit spanning tree information. • Use Global Settings—Select to use the settings defined in the STP Status and Global Settings, on page 165 page. • Filtering—Filters BPDU packets when Spanning Tree is disabled on an interface. • Flooding—Floods BPDU packets when Spanning Tree is disabled on an interface.
Path Cost	Set the port contribution to the root path cost or use the default cost generated by the system.
Priority	Set the priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority is a value 0–240, and must be a multiple of 16.
Port State	Displays the current STP state of a port. • Disabled—STP is currently disabled on the port. The port forwards traffic while learning MAC addresses. • Blocking—The port is currently blocked, and can't forward traffic (except for BPDU data) or learn MAC addresses. • Listening—The port is in Listening mode. The port can't forward traffic, and can't learn MAC addresses. • Learning—The port is in Learning mode. The port can't forward traffic, but it can learn new MAC addresses. • Forwarding—The port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
Designated Bridge ID	Displays the bridge priority and the MAC address of the designated bridge
Designated Port ID	Displays the priority and interface of the selected port.
Designated Cost	Displays the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
Forward Transitions	Displays the number of times the port has changed from the Blocking state to Forwarding state.
Speed	Displays the speed of the port.
LAG	Displays the LAG to which the port belongs. If a port is a member of a LAG, the LAG settings override the port settings.

Step 4 Click **Apply**. The interface settings are written to the Running Configuration file.

RSTP Interface Settings

Rapid Spanning Tree Protocol (RSTP) enables a faster STP convergence without creating forwarding loops.

The RSTP Interface Settings page enables you to configure RSTP per port. Any configuration that is done on this page is active when the global STP mode is set to RSTP.

To enter RSTP settings, proceed with the following steps:

Procedure

Step 1 Click **Spanning Tree** > **STP Status and Global Settings**.

Step 2 Enable RSTP.

Step 3 Click **Spanning Tree** > **RSTP Interface Settings**. The RSTP Interface Settings page appears.

Step 4 Select a port.

Note
Activate Protocol Migration is only available after selecting the port that is connected to the bridge partner being tested.

Step 5 If a link partner is discovered by using STP, click **Activate Protocol Migration** to run a Protocol Migration test. This discovers whether the link partner using STP still exists, and if so whether it has migrated to RSTP or MSTP. If it still exists as an STP link, the device continues to communicate with it by using STP. Otherwise, if it has been migrated to RSTP or MSTP, the device communicates with it using RSTP or MSTP, respectively.

Step 6 Select an interface, and click **Edit**.

Step 7 Enter the parameters:

Interface	Set the interface, and specify the port or LAG where RSTP is to be configured.
Point to Point Administrative Status	Define the point-to-point link status. Ports defined as Full Duplex are considered Point-to-Point port links. • Enabled-This port is an RSTP edge port when this feature is enabled, and is brought to Forwarding mode quickly (usually within 2 seconds). • Disabled-The port isn't considered point-to-point for RSTP purposes, which means that STP works on it at regular speed, as opposed to high speed. • Auto-Automatically determines the device status by using RSTP BPDUs.
Point to Point Operational Status	Displays the Point-to-Point operational status if the Point to Point Administrative Status is set to Auto.

Role	Displays the role of the port that was assigned by STP to provide STP paths. The possible roles are: • Root-Lowest cost path to forward packets to the Root Bridge. • Designated-The interface through which the bridge is connected to the LAN, which provides the lowest cost path from the LAN to the Root Bridge. • Alternate-Provides an alternate path to the Root Bridge from the root port. • Backup-Provides a backup path to the designated port path toward the Spanning Tree leaves. This provides a configuration in which two ports are connected in a loop by a point-to-point link. Backup ports are also used when a LAN has two or more established connections to a shared segment. • Disabled-The port is not participating in Spanning Tree.
Mode	Displays the current Spanning Tree mode: Classic STP or RSTP.
Fast Link Operational Status	Displays whether the Fast Link (Edge Port) is enabled, disabled, or automatic for the interface. The values are: • Enabled-Fast Link is enabled. • Disabled-Fast Link is disabled. • Auto-Fast Link mode is enabled a few seconds after the interface becomes active.
Port Status	Displays the RSTP status on the specific port. • Disabled-STP is currently disabled on the port. • Discarding-The port is currently discarding/blocked, and it cannot forward traffic or learn MAC addresses. • Listening-The port is in Listening mode. The port cannot forward traffic, and cannot learn MAC addresses. • Learning-The port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses. • Forwarding-The port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.

Step 8 Click **Apply**. The Running Configuration file is updated.

MSTP

Multiple Spanning Tree Protocol (MSTP) is used to separate the spanning tree protocol (STP) port state between various domains (on different VLANs). For example, while port A is blocked in one STP instance due to a loop on VLAN A, the same port can be placed in the Forwarding State in another STP instance. The MSTP Properties page enables you to define the global MSTP settings.

Multiple STP (MSTP) - MSTP is based on RSTP. It detects Layer 2 loops, and attempts to mitigate them by preventing the involved port from transmitting traffic. Since loops exist on a per-Layer 2-domain basis, a situation can occur when a port is blocked to eliminate a STP loop. Traffic will be forwarded to the port that is not blocked, and no traffic will be forwarded to the port that is blocked. This is not an efficient usage of bandwidth as the blocked port will always be unused. MSTP solves this problem by enabling several STP instances, so that it is possible to detect and mitigate loops separately in each instance. This enables a port to be blocked for one or more STP instances but non blocked for other STP instances. If different VLANs are associated with different STP instances, then their traffic will be relayed based on the STP port state of their associated MST instances. Better bandwidth utilization results.

MSTP Properties

The global MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree instance. MSTP enables formation of MST regions that can run multiple MST instances (MSTI). Multiple regions and other STP bridges are interconnected using one single common spanning tree (CST).

MSTP is fully compatible with RSTP bridges, in that an MSTP BPDU can be interpreted by an RSTP bridge as an RSTP BPDU. This not only enables compatibility with RSTP bridges without configuration changes, but also causes any RSTP bridges outside of an MSTP region to see the region as a single RSTP bridge, regardless of the number of MSTP bridges inside the region itself. For two or more switches to be in the same MST region, they must have the same VLANs to MST instance mapping, configuration revision number, and region name. Switches intended to be in the same MST region are never separated by switches from another MST region. If they are separated, the region becomes two separate regions.

This mapping can be done in the MSTP Instance Settings, on page 172. Use this page if the system operates in MSTP mode.

To define MSTP, follow these steps:

Procedure

Step 1 Click **Spanning Tree** > **MSTP** > **MSTP Properties**.

Step 2 Enter the parameters.

- Region Name—Define an MSTP region name.
- Revision—Define an unsigned 16-bit number that identifies the revision of the current MST configuration. The field range is 0–65535.
- Max Hops—Set the total number of hops that occur in a specific region before the BPDU is discarded. Once the BPDU is discarded, the port information is aged out. The field range is 1–40.
- IST Active—Displays the active regions.

Step 3 Click **Apply**. The MSTP properties are defined, and the Running Configuration file is updated.

MSTP Instance Settings

The MSTP Instance Settings page enables you to configure and view parameters per MST instance. This is the per-instance equivalent to the Configuring STP Status and Global Settings.

To enter the MSTP instance settings, proceed as follows:

Procedure

Step 1 Click **Spanning Tree** > **MSTP** >**MSTP Instance Settings**.

Step 2 Enter the parameters.

- Instance ID-Select an MST instance to be displayed and defined.
- Included VLAN-Displays the VLANs mapped to the selected instance. The default mapping is that all VLANs are mapped to the common and internal spanning tree (CIST) instance 0).
- Bridge Priority-Set the priority of this bridge for the selected MST instance.
- Designated Root Bridge ID-Displays the priority and MAC address of the Root Bridge for the MST instance.
- Root Port-Displays the root port of the selected instance.
- Root Path Cost-Displays the root path cost of the selected instance.
- Bridge ID-Displays the bridge priority and the MAC address of this device for the selected instance.
- Remaining Hops-Displays the number of hops remaining to the next destination.

Step 3 Click **Apply**. The MST Instance configuration is defined, and the Running Configuration file is updated.

MSTP Interface Settings

The MSTP Interface Settings page enables you to configure the port MSTP settings for every MST instance, and to view information that has currently been learned by the protocol, such as the designated bridge per MST instance.

To configure the ports in an MST instance, follow these steps:

Procedure

Step 1 Click **Spanning Tree** > **MSTP** > **MSTP Interface Settings**.

Step 2 Enter the parameters.

- Instance equals to—Select the MSTP instance to be configured.
- Interface Type equals to—Select whether to display the list of ports or LAGs.

Step 3 Click **Go**. The MSTP parameters for the interfaces on the instance are displayed.

Step 4 Select an interface, and click **Edit**.

Step 5 Enter the parameters.

Option	Description
Instance ID	Select the MST instance to be configured.
Interface	Select the interface for which the MSTI settings are to be defined.
Interface Priority	Set the port priority for the specified interface and MST instance.
Path Cost	Enter the port contribution to the root path cost in the User Defined textbox or select **Use Default** to use the default value.
Port State	Displays the MSTP status of the specific port on a specific MST instance. The parameters are defined as: • Disabled—STP is currently disabled. • Discarding—The port on this instance is currently discarding/blocked, and cannot forward traffic (with the exception of BPDU data) or learn MAC addresses. • Listening—The port on this instance is in Listening mode. The port cannot forward traffic, and cannot learn MAC addresses. • Learning—The port on this instance is in Learning mode. The port cannot forward traffic, but it can learn new MAC addresses. • Forwarding—The port on this instance is in Forwarding mode. The port can forward traffic and learn new MAC addresses. • Boundary—The port on this instance is a boundary port. It inherits its state from instance 0 and can be viewed on the STP Interface Settings, on page 166.
Port Role	Displays the port or LAG role, per port or LAG per instance, assigned by the MSTP algorithm to provide STP paths: • Root—Forwarding packets through this interface provides the lowest cost path for forwarding packets to the root device. • Designated Port—The interface through which the bridge is connected to the LAN, which provides the lowest root path cost from the LAN to the Root Bridge for the MST instance. • Alternate—The interface provides an alternate path to the Root Bridge from the root port. • Backup—The interface provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more established connections to a shared segment. • Disabled—The interface does not participate in the Spanning Tree. • Boundary—The port on this instance is a boundary port. It inherits its state from instance 0 and can be viewed on the STP Interface Settings, on page 166.
Mode	Displays the current interface Spanning Tree mode. • If the link partner is using MSTP or RSTP, the displayed port mode is RSTP.

Option	Description
	• If the link partner is using STP, the displayed port mode is STP.
Type	Displays the MST type of the port. • Boundary—A Boundary port attaches MST bridges to a LAN in a remote region. If the port is a boundary port, it also indicates whether the device on the other side of the link is working in RSTP or STP mode. • Internal—The port is an internal port.
Designated Bridge ID	Displays the ID number of the bridge that connects the link or shared LAN to the root.
Designated Port ID	Displays the Port ID number on the designated bridge that connects the link or the shared LAN to the root.
Designated Cost	Displays the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
Remain Hops	Displays the hops remaining to the next destination.
Forward Transitions	Displays the number of times the port has changed from the Forwarding state to the Discarding state.

Step 6 Click **Apply**. The Running Configuration file is updated.

VLANs to MSTP Instance

The VLAN to MSTP Instance page enables you to map each VLAN to a Multiple Spanning Tree Instance (MSTI). For devices to be in the same region, they must have the same mapping of VLANs to MSTIs.

Note The same MSTI can be mapped to more than one VLAN, but each VLAN can only have one MST instance attached to it. Configuration on this page (and all of the MSTP pages) applies if the system STP mode is MSTP. Up to 16 MST instances can be defined in addition to instance zero. For those VLANs that aren't explicitly mapped to one of the MST instances, the device automatically maps them to the CIST (Core and Internal Spanning Tree) instance. The CIST instance is MST instance 0.

To map VLANs to MST Instances, follow these steps:

Procedure

Step 1 Click **Spanning Tree** > **MSTP** > **VLANs to MSTP Instance**.

The VLAN to MSTP Instance page displays the following fields:

• MSTP Instance ID-All MST instances are displayed.

- VLANs-All VLANs belonging to the MST instance are displayed.

Step 2 To add a VLAN to an MSTP instance, select the MST instance, and click **Edit**.

Step 3 Enter the parameters:

- MSTP Instance ID-Select the MST instance.
- VLANs-Define the VLANs being mapped to this MST instance.
- Action-Define whether to Add (map) the VLAN to the MST instance or Remove it.

Step 4 Click **Apply**. The MSTP VLAN mappings are defined, and the Running Configuration file is updated.

PVST

Per VLAN Spanning Tree (PVST) is a protocol running a separate instance of the 802.1Q STP standard protocol per each VLAN configured on the device. RSTP standard protocol per each VLAN configured on the device. The PVST protocol is a protocol that was designed to address the problem that exist with STP/RSTP standard based implementation - that in some cases a port that is in blocking mode (for more than 1 VLANs) may create an efficient usage of bandwidth since it cannot be used for any traffic forwarding.

PVST addresses this issue by assigning a separate spanning tree instance for each VLAN configured on the device. Up to 126 PVST instances are supported. this means that if more than 126 VLANs are configured on the device, PVST cannot be enabled. Likewise, if PVST is enabled you cannot configure more than 126 VLANs

The device supports the PVST/RPVST Plus flavor of the protocols. This section refers to PVST to describe both PVST+ and RPVST+ feature behavior.

PVST VLAN Settings

To define the PVST VLAN settings, follow these steps:

Procedure

Step 1 Click **Spanning Tree > PVST > PVST VLAN Settings**.

The PVST VLAN Settings page enables you to configure PVST settings for each VLAN ID that is configured on the device, except the VLAN ID 1.

To configure the PVST parameters on an interface:

Step 2 Select a row in the table and click **Copy Settings** to create an new PVST VLAN based on the selected row, or click **Edit** to revise the selected row.

Note
VLAN entry 1 cannot be edited. Edit the values of the PVST VLAN as needed:

- VLAN ID—the VLAN ID of the PVST instance

- Priority—The PVST VLAN STP priority value.
- Address—The address of the VLAN
- Hello Time—The interval (in seconds) that a Root Bridge waits between configuration messages.
- Max Age—The interval (in seconds) that this VLAN STP instance can wait without receiving a configuration message, before attempting to redefine its own configuration.
- Forward Delay—The interval (in seconds) that this VLAN STP instance remains in a learning state before forwarding packets.

Step 3 Click **Details** to view the PVST VLAN details.

- VLAN ID—the VLAN ID of the PVST instance
- Root Priority—The PVST VLAN STP priority value.
- Root Hello Time—The interval (in seconds) that a Root Bridge waits between configuration messages.
- Root Max Age—The interval (in seconds) that this VLAN STP instance can wait without receiving a configuration message, before attempting to redefine its own configuration.
- Root Forward Delay—The interval (in seconds) that this VLAN STP instance remains in a learning state before forwarding packets.
- Root Port—The port that offers the lowest cost path on this VLAN from this bridge to the root.
- Root Path Cost—The cost, on this VLAN of the path from this bridge to the root.
- Root Bridge ID—The bridge ID of the root bridge in this VLAN.
- Bridge ID—The bridge ID of this device and VLAN.
- Topology Change Count—The total number of STP topology changes that have occurred on this VLAN last topology change.
- Last Topology Change— Details of when the last topology was changed.

Step 4 Click **Apply**. The new/revised PVST VLAN is added/updated.

PVST Interface Settings

The PVST Interface Settings page enables you to configure PVST on a per-port and VLAN basis, and to view the information learned by the protocol, such as the designated bridge.

To configure the PVST parameters on an interface, proceed as follows:

Procedure

Step 1 Click **Spanning Tree > PVST > PVST Interface Settings.**

Step 2 Using the filters, select the VLAN ID and Interface Type (Port or Lag) from the drop-down list and click **Go**. Then, the following PVST interface information will be displayed for each VLAN PVST.

Option	Description
Interface	The interface name.
Priority	The priority value of the port for this VLAN instance. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority is a value 0–240, and must be a multiple of 16.
Port Cost	The port contribution, per VLAN instance, to the root path cost or use the default cost generated by the system.
State	Displays the current STP state of a port, per VLAN instance. • Disabled—PVST is currently disabled on the port. The port forwards traffic while learning MAC addresses. • Blocking—The port is blocked for this VLAN instance and can't forward traffic (except for BPDU data) or learn MAC addresses. • Listening—The port is in Listening state for this VLAN instance. The port can't forward traffic, and can't learn MAC addresses. • Learning—The port is in Learning state for this VLAN instance. The port can't forward traffic, but it can learn new MAC addresses. • Forwarding—The port is in Forwarding state for this VLAN instance. The port can forward traffic and learn new MAC addresses.
Role	Displays the PVST role, per PVST instance, assigned by the PVST algorithm to provide STP path. • Root—Forwarding packets through this interface provides the lowest cost path for forwarding packets to the root device. • Designated—The interface through which the bridge is connected to the LAN, which provides the lowest root path cost from the LAN to the Root Bridge for the PVST instance. • Alternate—The interface provides an alternate path to the root device from the root interface. • Backup—The interface provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more established connections to a shared segment. • Disable—The interface doesn't participate in the Spanning Tree.
Mode	Displays the PVST mode. • RPVST—The port is running the RPVST+ flavor of PVST. • PVST—The port is running the PVST+ flavor of PVST.
Inconsistency	Displays the inconsistency.

Option	Description
Designated Bridge ID	Displays the bridge priority and the MAC address of the designated bridge for the current VLAN instance.
Designated Port ID	Displays the priority and interface of the selected port for the current VLAN instance.
Designated Cost	Displays the cost of the port participating in the STP topology for the current VLAN instance. Ports with a lower cost are less likely to be blocked if STP detects loops
Forward Transitions	Displays the number of times the port has changed from the Blocking state to Forwarding state for the current VLAN instance.

Step 3 Select an interface and click **Edit**, to edit the Interface type, Priority, or Path Cost of the selected VLAN,

To copy the configuration settings of the selected port to the other ports in the current VLAN click **Copy Settings to Ports...**

To copy the port configuration settings to the same ports in a range of other VLANs, click **Copy Settings to VLANs...**.

Step 4 Enter the parameters.

Step 5 Click **Apply**. The interface settings are written to the Running Configuration file.

Step 6 Click **Apply to all existing VLANs** to apply the settings to all the VLANs created on the switch.

PVST Inconsistent Ports

The PVST Inconsistent Ports page displays the inconsistent PVST ports.

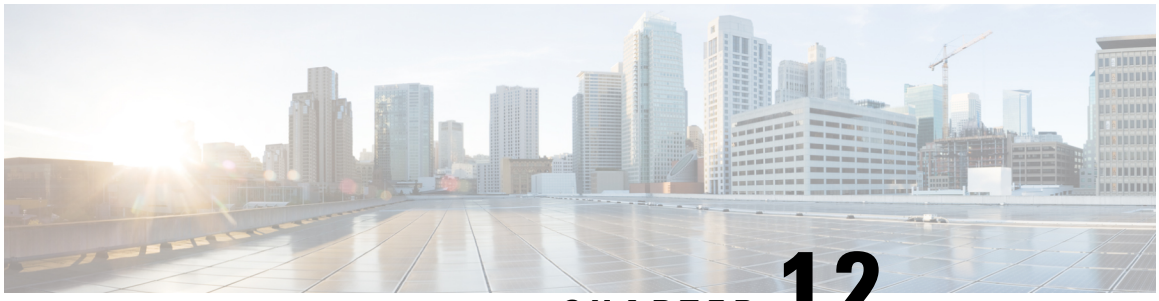
To view inconsistent PVST ports, follow these steps:

Procedure

Click **Spanning Tree > PVST > PVST Inconsistent Ports**.

This page displays details on ports that are in the PVST inconsistent state:

- VLAN ID—the VLAN ID of the PVST instance
- Interface Name—The interface ID
- Inconsistency—Displays the inconsistency state.



CHAPTER 12

MAC Address Tables

This chapter contains the following sections:

- Static Addresses, on page 179
- Dynamic Address Settings, on page 180
- Dynamic Addresses, on page 180
- Reserved MAC Addresses, on page 181

Static Addresses

Static MAC addresses are assigned to a specific physical interface and VLAN on the device. If that address is detected on another interface, it's ignored, and isn't written to the address table.

To define a static address, follow these steps:

Procedure

Step 1 Click **MAC Address Tables** > **Static Addresses**.

The Static Addresses page contains the currently defined static addresses.

Step 2 Click **Add**.

Step 3 Enter the parameters.

- VLAN ID—Select the VLAN ID for the port.
- MAC Address—Enter the interface MAC address.
- Interface—Select an interface for the entry.
- Status—Select how the entry is treated. The options are:
  - Permanent—The system never removes this MAC address. If the static MAC address is saved in the Startup Configuration, it's retained after rebooting.
  - Delete on reset—The static MAC address is deleted when the device is reset.
  - Delete on timeout—The MAC address is deleted when aging occurs.
  - Secure—The MAC address is secure when the interface is in classic locked mode.

Step 4 Click **Apply**. A new entry appears in the table.

Step 5 To delete a static address, click the **Delete** icon and then click **Apply** to save the new settings.

Dynamic Address Settings

The Dynamic Address Table (bridging table) contains the MAC addresses acquired by monitoring the source addresses of frames entering the device. To prevent this table from overflowing and to make room for new MAC addresses, an address is deleted if no corresponding traffic is received for a certain period of time known as the aging time.

To configure the aging time for dynamic addresses, follow these steps:

Procedure

Step 1 Click **MAC Address Tables** > **Dynamic Address Settings**.

Step 2 Enter Aging Time. The aging time is a value between the user-configured value and twice that value minus 1. For example, if you entered 300 seconds, the aging time is between 300 and 599 seconds.

Step 3 Click **Apply**. The aging time is updated.

Dynamic Addresses

To query dynamic addresses, follow these steps:

Procedure

Step 1 Click **MAC Address Tables** > **Dynamic Addresses**.

Step 2 In the Filter block, you can enter the following query criteria:

- VLAN ID—Enter the VLAN ID for which the table is queried.
- MAC Address—Enter the MAC address for which the table is queried.
- Interface—Select the interface for which the table is queried. The query can search for specific ports, or LAGs.

Step 3 Click **Go**. The Dynamic MAC Address Table is queried and the results are displayed.

Step 4 To delete all of the dynamic MAC addresses. click **Clear Table**.

Reserved MAC Addresses

When the device receives a frame with a destination MAC address that belongs to a reserved range (per the IEEE standard), the frame can be discarded or bridged. The entry in the Reserved MAC Address Table can either specify the reserved MAC address or the reserved MAC address and a frame type:

To add an entry for a reserved MAC address, proceed as follows:

Procedure

Step 1 Click **MAC Address Tables** > **Reserved MAC Addresses**.

The reserved MAC addresses are displayed. The fields are described in the Add page, except for the following field:

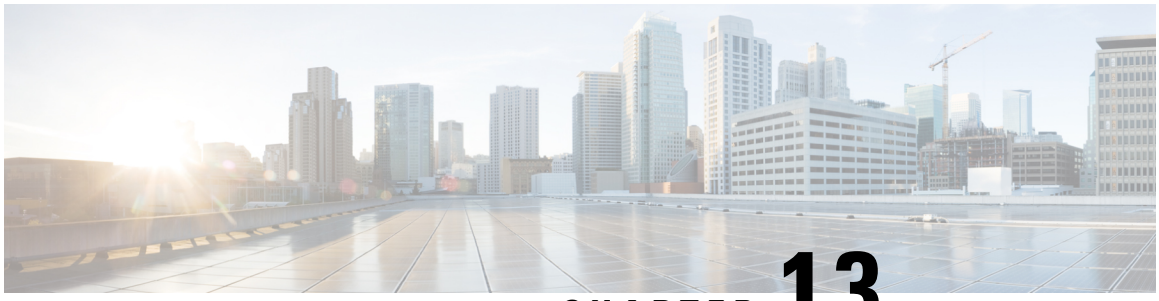
Protocol—Displays the protocol supported on the device (called Peer),

Step 2 Click **Add**.

Step 3 Enter the values for the following fields:

- MAC Address—Select the MAC address to be reserved.
- Frame Type—Select a frame type based on the following criteria:
  - Ethernet V2—Applies to Ethernet V2 packets with the specific MAC address.
  - LLC—Applies to Logical Link Control (LLC) packets with the specific MAC address.
  - LLC-SNAP—Applies to Logical Link Control/Sub-Network Access Protocol (LLC-SNAP) packets with the specific MAC address.
  - All—Applies to all packets with the specific MAC address.
- Action—Select one of the following actions to be taken upon receiving a packet that matches the selected criteria:
  - Bridge—Forward the packet to all VLAN members
  - Discard—Delete the packet.

Step 4 Click **Apply**. A new MAC address is reserved.



CHAPTER 13

Multicast

This chapter contains the following sections:

- Multicast Properties, on page 183
- MAC Group Address, on page 184
- IP Multicast Group Address, on page 186
- IPv4 Multicast Configuration, on page 187
- IPv6 Multicast Configuration, on page 192
- IGMP/MLD Snooping IP Multicast Group, on page 196
- Multicast Router Port, on page 197
- Forward All, on page 198
- Unregistered Multicast, on page 198

Multicast Properties

Multicast forwarding enables one-to-many information dissemination. Multicast applications are useful for dissemination of information to multiple clients, where clients do not require reception of the entire content. A typical application is a cable-TV-like service, where clients can join a channel in the middle of a transmission, and leave before it ends.

The data is sent only to relevant ports. Forwarding the data only to the relevant ports conserves bandwidth and host resources on links. By default, all Multicast frames are flooded to all ports of the VLAN. It is possible to selectively forward only to relevant ports and filter (drop) the Multicast on the rest of the ports by enabling the Bridge Multicast filtering status in this section.

Multicast addresses have the following properties:

- Each IPv4 Multicast address is in the address range 224.0.0.0 to 239.255.255.255.
- The IPv6 Multicast address is FF00:/8.
- To map an IP Multicast group address to an Layer 2 Multicast address:

For IPv4, this is mapped by taking the 23 low-order bits from the IPv4 address, and adding them to the 01:00:5e prefix. By standard, the upper nine bits of the IP address are ignored, and any IP addresses that only differ in the value of these upper bits are mapped to the same Layer 2 address, since the lower 23 bits that are used are identical. For example, 234.129.2.3 is mapped to a MAC Multicast group address 01:00:5e:01:02:03. Up to 32 IP Multicast group addresses can be mapped to the same Layer 2 address.

For IPv6, this is mapped by taking the 32 low-order bits of the Multicast address, and adding the prefix of 33:33. For example, the IPv6 Multicast address FF00::1122:3344 is mapped to Layer 2 Multicast 33:33:11:22:33:44.

To enable Multicast filtering, and select the forwarding method, follow these steps:

Procedure

Step 1 Click **Multicast** > **Properties**.

Step 2 Enter the parameters.

Bridge Multicast Filtering Status	Select to enable filtering.
VLAN ID	Select the VLAN ID to set its forwarding method.
Forwarding Method for IPv6	Set one of the following forwarding methods for IPv6 addresses: • MAC Group Address—Forward packets according to the MAC Multicast group address • IP Group Address—Forward packets according to the IPv6 Multicast group address • Source-Specific IP Group Address—Forward packets according to the source IPv6 and IPv6 Multicast group address. If an IPv6 address is configured on the VLAN, the operational forwarding methods for IPv6 Multicast are IP Group Address. **Note** For IPv6 IP Group and Source-Specific IP Group Address modes, the device checks a match only for 4 bytes of the destination Multicast and source address. For the destination Multicast address, the last 4 bytes of group ID are matched. For the source address, the last 3 bytes + the 5th from the last byte are matched.
Forwarding Method for IPv4	Set one of the following forwarding methods for IPv4 addresses: • MAC Group Address—Forward packets according to the MAC Multicast group address • IP Group Address—Forward packets according to the IPv4 Multicast group address • Source-Specific IP Group Address—Forward packets according to the source IPv4 and IPv4 Multicast group address. If an IPv4 address is configured on the VLAN, the operational forwarding method for IPv4 Multicast are IP Group Address.

Step 3 Click **Apply**. The Running Configuration file is updated.

MAC Group Address

The MAC Group Address page has the following functions:

- Query and view information from the Multicast Forwarding Data Base (MFDB), relating to a specific VLAN ID or a specific MAC address group This data is acquired either dynamically through IGMP/MLD snooping or statically by manual entry.
- Add or delete static entries to the MFDB that provide static forwarding information, based on MAC destination addresses.
- Displays all ports/LAGs that are members of each VLAN ID and MAC address group.

To define and view MAC Multicast groups, follow these steps:

Procedure

Step 1 Click **Multicast** > **MAC Group Address**.

Step 2 Enter the Filter parameters.

- VLAN ID equals to—Set the VLAN ID of the group to be displayed.
- MAC Group Address equals to—Set the MAC address of the Multicast group to be displayed. If no MAC Group Address is specified, the page contains all the MAC Group Addresses from the selected VLAN.

Step 3 Click **Go,** and the MAC Multicast group addresses are displayed in the lower block.

Step 4 Click **Add** to add a static MAC Group Address.

Step 5 Enter the parameters.

- VLAN ID—Defines the VLAN ID of the new Multicast group.
- MAC Group Address—Defines the MAC address of the new Multicast group.

Step 6 Click **Apply**, the MAC Multicast group is saved to the Running Configuration file.

To configure and display the registration for the interfaces within the group, select an address, and click **Details.**

The page displays:

- VLAN ID—The VLAN ID of the Multicast group.
- MAC Group Address—The MAC address of the group.

Step 7 Select either port or LAG from the Filter: Interface Type menu.

Step 8 Click **Go** to display the port or LAG membership of the VLAN.

Step 9 Select the way that each interface is associated with the Multicast group:

- Static—Attaches the interface to the Multicast group as a static member.
- Dynamic—Indicates that the interface was added to the Multicast group as a result of IGMP/MLD snooping.
- Forbidden—Specifies that this port isn't allowed to join this Multicast group on this VLAN.
- None—Specifies that the port isn't currently a member of this Multicast group on this VLAN.

Step 10 Click **Apply**, and the Running Configuration file is updated.

IP Multicast Group Address

The IP Multicast Group Address page is similar to the MAC Group Address page except that Multicast groups are identified by IP addresses. The IP Multicast Group Address page enables querying and adding IP Multicast groups.

To define and view IP Multicast groups, follow these steps:

Procedure

Step 1 Click **Multicast** > **IP Multicast Group Address**.

The page contains all of the IP Multicast group addresses learned by snooping.

Step 2 Enter the parameters required for filtering.

- VLAN ID equals to—Define the VLAN ID of the group to be displayed.
- IP Version equals to—Select IPv6 or IPv4.
- IP Multicast Group Address equals to—Define the IP address of the Multicast group to be displayed. This is only relevant when the Forwarding mode is (S,G).
- Source IP Address equals to—Define the source IP address of the sending device. If mode is (S,G), enter the sender S. This together with the IP Group Address is the Multicast group ID (S,G) to be displayed. If mode is (*.G), enter an * to indicate that the Multicast group is only defined by destination.

Step 3 Click **Go**. The results are displayed in the lower block.

Step 4 Click **Add** to add a static IP Multicast Group Address.

Step 5 Enter the parameters.

- VLAN ID—Defines the VLAN ID of the group to be added.
- IP Version—Select the IP address type.
- IP Multicast Group Address—Define the IP address of the new Multicast group.
- Source Specific—Indicates that the entry contains a specific source, and adds the address in the IP Source Address field. If not, the entry is added as a (*, G) entry, an IP group address from any IP source.
- Source IP Address—Defines the source address to be included.

Step 6 Click **Apply**. The IP Multicast group is added, and the device is updated.

Step 7 To configure and display the registration of an IP group address, select an address and click **Details**.

The VLAN ID, IP Version, IP Multicast Group Address, and Source IP Address selected are displayed as read-only in the top of the window. You can select the filter type:

- Interface Type equals to—Select whether to display ports or LAGs.

Step 8 For each interface, select its association type. The options are as follows:

- Static—Attaches the interface to the Multicast group as a static member.

- Dynamic—Attaches the interface to the Multicast group as a dynamic member.
- Forbidden—Specifies that this port is forbidden from joining this group on this VLAN.
- None—Indicates that the port isn't currently a member of this Multicast group on this VLAN. This is selected by default until Static or Forbidden is selected.

Step 9 Click **Apply**. The Running Configuration file is updated.

IPv4 Multicast Configuration

A multicast address is a single IP data packet set that represents a network host group. Multicast addresses are available to process datagrams or frames intended to be multicast to a designated network service. Multicast addressing is applied in the link layer (Layer 2 of the OSI Model) and the Internet layer (Layer 3 of the OSI Model) for IP versions 4 (IPv4) and 6 (IPv6).

Multicast addresses in IPV4 are defined using leading address bits of 1110, which originate from the classful network design of the early Internet when this group of addresses was designated as Class D.

IPv4 multicast packets are delivered using the Ethernet MAC address range 01:00:5e:00:00:00–01:00:5e:7f:ff:ff. This range has 23 bits of available address space. The first octet (01) includes the broadcast/multicast bit. The lower 23 bits of the 28-bit multicast IP address are mapped into the 23 bits of available Ethernet address space. This means that there is ambiguity in delivering packets. If two hosts on the same subnet each subscribe to a different multicast group whose address differs only in the first 5 bits, Ethernet packets for both multicast groups will be delivered to both hosts, requiring the network software in the hosts to discard the unrequired packets.

This section covers how to configure the IPv4 multicast.

IGMP Snooping

To support selective IPv4 Multicast forwarding, bridge Multicast filtering must be enabled (in Multicast Properties, on page 183). The IGMP Snooping must be enabled globally and for each relevant VLAN in the IGMP Snooping page.

To enable IGMP Snooping and identify the device as an IGMP Snooping Querier on a VLAN, follow these steps:

Procedure

Step 1 Click **Multicast** > **IPv4 Multicast Configuration** > **IGMP Snooping**.

- IGMP Snooping Status—Select to enable IGMP snooping globally on all interfaces.
- IGMP Querier Status—Select to enable IGMP querier globally on all interfaces.

Step 2 IGMP Snooping is only operational when Bridge Multicast Filtering is enabled. You can enable it here: Multicast Properties, on page 183.

Step 3 To configure IGMP on an interface, select a static VLAN and click **Edit**. Enter the following fields:

Option	Description
VLAN ID	Select The VLAN Id from the dropdown list.
IGMP Snooping Status	Select to enable IGMP Snooping on the VLAN. The device monitors network traffic to determine which hosts have asked to be sent Multicast traffic.
MRouter Ports Auto Learn	Select to enable Auto Learn of the Multicast router.
Immediate Leave	Select to enable the switch to remove an interface that sends a leave message from the forwarding table without first sending out MAC-based general queries to the interface. When an IGMP Leave Group message is received from a host, the system removes the host port from the table entry. After it relays the IGMP queries from the Multicast router, it deletes entries periodically if it doesn't receive any IGMP membership reports from the Multicast clients. When enabled, this feature reduces the time it takes to block unnecessary IGMP traffic sent to a device port.
Last Member Query Counter	Number of MLD group-specific queries sent before the device assumes that there are no more members for the group, if the device is the elected querier. • Use Query Robustness (x)—The number in parentheses is the current query robustness value. • User Defined—Enter a user-defined value.
IGMP Querier Status	Select to enable this feature. This feature is required if there's no Multicast router.
IGMP Querier Election	IGMP Querier Election—Whether the IGMP querier election is enabled or disabled. If the IGMP Querier election mechanism is enabled, the IGMP Snooping querier supports the standard IGMP Querier election mechanism specified in RFC3810. If the IGMP Querier election mechanism is disabled, the IGMP Snooping querier delays sending General Query messages for 60 seconds after it was enabled, and if there's no other querier, it starts sending General Query messages. It stops sending General Query messages when it detects another querier. The IGMP Snooping Querier resumes sending General Query messages if it does hear another querier for a Query Passive interval that equals: Robustness * (Query Interval) + 0.5 * Query Response Interval.
IGMP Querier Version	Select the IGMP version to be used if the device becomes the elected querier. Select IGMPv3 if there are switches and/or Multicast routers in the VLAN that perform source-specific IP Multicast forwarding. Otherwise, select IGMPv2.
Querier Source IP Address	The IP address of the device source interface to be used in messages sent. In MLD this address is selected automatically by the system. • Auto—The system takes the source IP address from the IP address defined on the outgoing interface. • User Defined—Enter a user-defined IP address.

Step 4 Click **Apply**. The Running Configuration file is updated.

Note Changes in IGMP Snooping timers configuration, such as: Query Robustness, Query Interval etc. don't take effect on timers which already created.

IGMP Interface Settings

An interface that is defined as a Multicast router port receives all IGMP packets (reports and queries) and all Multicast data.

To define IGMP on an interface, complete the following steps:

Procedure

Step 1 Click **Multicast** > **IPv4 Multicast Configuration** > **IGMP Interface Settings**.

The following fields are displayed for each interface on which IGMP is enabled:

- Interface Name—Interface on which IGMP snooping is defined.
- Router IGMP Version—IGMP version.
- Query Robustness—Enter the number of expected packet losses on a link
- Query Interval (sec)—Interval between the General Queries to be used if this device is the elected querier.
- Query Max Response Interval (sec)—Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.
- Last Member Query Interval (msec)—Maximum Response Delay to be used if the device can't read Max Response Time value from group-specific queries sent by the elected querier.
- Multicast TTL Threshold—Enter the Time-to-Live (TTL) threshold of packets being forwarded on an interface.

  Multicast packets with a TTL value less than the threshold aren't forwarded on the interface.

  The default value of 0 means that all Multicast packets are forwarded on the interface.

  A value of 256 means that no Multicast packets are forwarded on the interface.

  Configure the TTL threshold only on border routers. Conversely, routers on which you configure a TTL threshold value automatically become border routers.

Step 2 Select an interface, and click **Edit**. Enter the values of the fields described above.

Step 3 Click **Apply**. The Running Configuration file is updated.

IGMP VLAN Settings

To configure IGMP on a specific VLAN, complete the following steps:

Procedure

Step 1 Click **Multicast** > **IPv4 Multicast Configuration** > **IGMP VLAN Settings**.

The following fields are displayed for each VLAN on which IGMP is enabled:

- Interface Name—VLAN on which IGMP snooping is defined.
- Router IGMP Version—Version of IGMP Snooping.
- Query Robustness—Enter the number of expected packet losses on a link.
- Query Interval (sec)—Interval between the General Queries to be used if this device is the elected querier.
- Query Max Response Interval (sec)—Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.
- Last Member Query Interval (msec)—Enter the Maximum Response Delay to be used if the device can't read Max Response Time value from group-specific queries sent by the elected querier.
- Multicast TTL Threshold—Enter the Time-to-Live (TTL) threshold of packets being forwarded on an interface.

  Multicast packets with a TTL value less than the threshold aren't forwarded on the interface.

  The default value of 0 means that all Multicast packets are forwarded on the interface.

  A value of 256 means that no Multicast packets are forwarded on the interface.

  Configure the TTL threshold only on border routers. Conversely, routers on which you configure a TTL threshold value automatically become border routers.

Step 2 Select an interface, and click **Edit**. Enter the values of the fields described above.

Step 3 Click **Apply**. The Running Configuration file is updated.

IGMP Proxy

Note IGMP Proxy is only operational if IPv4 routing is enabled in IPv4 Interface, on page 201.

To configure IGMP Proxy, follow these steps:

Procedure

Step 1 Click **Multicast** > **IPv4 Multicast Configuration** > **IGMP Proxy**.

Step 2 Enter the following global fields:

IGMP Multicast Routing	Select to enable IPv4 Multicast routing.
Downstream Protection	Select to discard downstream packets not required for the device.

Source Specific Multicast	Select to enable delivering Multicast packets originating from a specific source address defined in the next field.
SSM IPv4 Access List	Define the list containing source addresses from which to deliver Multicast packets: • Default list—Defines the SSM range access list to 232.0.0.0/8. • User-defined access list—Select the standard IPv4 access list name defining the SSM range.

Step 3 Click **Apply**. The Running Configuration file is updated.

Step 4 To add protection to a VLAN, click **Add** and enter the following fields:

Upstream Interface	Select the upstream interface. Since there's only a single upstream interface, if one has already been selected, this field is grayed out.
Downstream Interface	Select the downstream interface. There can be multiple downstream interfaces.
Downstream Protection	Select one of the following options: • Use global—Use the status set in the global block. • Disable—This enables forwarding of IPv4 Multicast traffic from downstream interfaces. • Enable—This disables forwarding from downstream interfaces.

Step 5 Click **Apply**. The Running Configuration file is updated.

The following fields are displayed for each IPv4 Multicast route:

Source Address	Unicast source IPv4 address.
Group Address	Multicast destination IPv4 address.
Incoming Interface	Expected interface for a Multicast packet from the source. If the packet isn't received on this interface, it's discarded.
Outgoing Interfaces	Interfaces through which packets will be forwarded.
Uptime	Length of time in hours, minutes, and seconds that the entry has been in the IP Multicast routing table.
Expiry Time	Length of time in hours, minutes, and seconds until the entry is removed from the IP Multicast routing table.

IPv6 Multicast Configuration

IP multicast is a method of sending Internet Protocol (IP) datagrams to a group of interested receivers in a single transmission. It is the IP-specific form of multicast and is used for streaming media and other network applications. It uses specially reserved multicast address blocks in IPv4 and IPv6.

Unicast packets are delivered to a specific recipient on an Ethernet or IEEE 802.3 subnet by setting a specific layer 2 MAC address on the Ethernet packet address. Broadcast packets make use of a broadcast MAC address (FF:FF:FF:FF:FF:FF). For IPv6 multicast addresses, the Ethernet MAC is derived by the four low-order octets OR'ed with the MAC 33:33:00:00:00:00, so for example the IPv6 address FF02:DEAD:BEEF::1:3 would map to the Ethernet MAC address 33:33:00:01:00:03.

This section covers how to configure the IPv6 multicast.

MLD Snooping

To support selective IPv6 Multicast forwarding, bridge Multicast filtering must be enabled (in the Multicast Properties, on page 183), and MLD Snooping must be enabled globally and for each relevant VLAN in the MLD Snooping pages.

To enable MLD Snooping and configure it on a VLAN, complete the following:

Procedure

Step 1 Click **Multicast** > **IPv6 Multicast Configuration** > **MLD Snooping**.

Note
MLD Snooping is only operational when Bridge Multicast Filtering is enabled and can be enabled here Multicast Properties, on page 183.

Step 2 Enable or disable the following features:

- MLD Snooping Status—Select to enable MLD snooping globally on all interfaces.
- MLD Querier Status—Select to enable MLD querier globally on all interfaces.

Step 3 To configure MLD proxy on an interface, select a static VLAN and click **Edit**. Enter the following fields:

Option	Description
MLD Snooping Status	Select to enable MLD Snooping on the VLAN. The device monitors network traffic to determine which hosts have asked to be sent Multicast traffic. The device performs MLD snooping only when MLD snooping and Bridge Multicast filtering are both enabled.
MRouter Ports Auto Learn	Select to enable Auto Learn of the Multicast router.
Immediate Leave	Select to enable the switch to remove an interface that sends a leave message from the forwarding table without first sending out MAC-based general queries to the interface. When an MLD Leave Group message is received from a host, the system removes the host port from the table entry. After it relays the MLD queries from the Multicast router, it deletes entries periodically if it does

Option	Description
	not receive any MLD membership reports from the Multicast clients. When enabled, this feature reduces the time it takes to block unnecessary MLD traffic sent to a device port.
Last Member Query Counter	Number of MLD group-specific queries sent before the device assumes there are no more members for the group, if the device is the elected querier. • Use Query Robustness (x)—The number in parentheses is the current query robustness value. • User Defined—Enter a user-defined value.
MLD Querier Status	Select to enable this feature. This feature is required if there is no Multicast router.
MLD Querier Election	Whether the MLD querier election is enabled or disabled. If the MLD Querier election mechanism is enabled, the MLD Snooping querier supports the standard MLD Querier election mechanism specified in RFC3810. If the MLD Querier election mechanism is disabled, the MLD Snooping querier delays sending General Query messages for 60 seconds after it was enabled, and if there is no other querier, it starts sending General Query messages. It stops sending General Query messages when it detects another querier. The MLD Snooping Querier resumes sending General Query messages if it does hear another querier for a Query Passive interval that equals: Robustness * (Query Interval) + 0.5 * Query Response Interval.
MLD Querier Version	Select the MLD version to be used if the device becomes the elected querier. Select MLDv2 if there are switches and/or Multicast routers in the VLAN that perform source-specific IP Multicast forwarding. Otherwise, select MLDv1.

Step 4 Click **Apply**. The Running Configuration file is updated.

Note Changes in MLD Snooping timers configuration, such as: Query Robustness, Query Interval etc. do not take effect on timers which already created.

MLD Interface Settings

An interface that is defined as a Multicast router port receives all MLD packets (reports and queries) and all Multicast data.

To configure an interface as a Multicast router interface, complete the following::

Procedure

Step 1 Click **Multicast** > **IPv6 Multicast Configuration** > **MLD Interface Settings**.

The following fields are displayed for each interface on which MLD is enabled:

- Router MLD Version—MLD version of the Multicast router.
- Query Robustness—Enter the number of expected packet losses on a link.
- Query Interval (sec)—Interval between the general queries to be used if this device is the elected querier.
- Query Max Response Interval (sec)—Delay used to calculate the Maximum Response Code inserted into the periodic general queries.
- Last Member Query Interval (msec)—Maximum Response Delay to be used if the device can't read Max Response Time value from group-specific queries sent by the elected querier.
- Multicast TTL Threshold—Enter the Time-to-Live (TTL) threshold of packets being forwarded on an interface.

  Multicast packets with a TTL value less than the threshold aren't forwarded on the interface.

  The default value of 0 means that all Multicast packets are forwarded on the interface.

  A value of 256 means that no Multicast packets are forwarded on the interface.

  Configure the TTL threshold only on border routers. Conversely, routers on which you configure a TTL threshold value automatically become border routers.

Step 2 To configure an interface, select it and click **Edit**. Enter the fields that are described above.

Step 3 Click **Apply**. The Running Configuration file is updated.

MLD VLAN Settings

To configure MLD on a specific VLAN, follow these steps:

Procedure

Step 1 Click **Multicast** > **IPv6 Multicast Configuration** > **MLD VLAN Settings**.

The following fields are displayed for each VLAN on which MLD is enabled:

- Interface Name—VLAN for which MLD information is being displayed.
- Router MLD Version—Version of MLD router.
- Query Robustness—Enter the number of expected packet losses on a link
- Query Interval (sec)—Interval between the General Queries to be used if this device is the elected querier.
- Query Max Response Interval (sec)—Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.
- Last Member Query Interval (msec)—Enter the Maximum Response Delay to be used if the device can't read Max Response Time value from group-specific queries sent by the elected querier.
- Multicast TTL Threshold—Enter the Time-to-Live (TTL) threshold of packets being forwarded on an interface.

  Multicast packets with a TTL value less than the threshold aren't forwarded on the interface.

  The default value of 0 means that all Multicast packets are forwarded on the interface.

A value of 256 means that no Multicast packets are forwarded on the interface.

Configure the TTL threshold only on border routers. Conversely, routers on which you configure a TTL threshold value automatically become border routers.

Step 2 To configure a VLAN, select it and click **Edit**. Enter the fields described above.

Step 3 Click **Apply**. The Running Configuration file is updated.

MLD Proxy



Note MLD Proxy is only operational if IPv6 routing is enabled in IPv6 Global Configuration, on page 227.

To configure MLD Proxy, follow these steps:

Procedure

Step 1 Click **Multicast > IPv6 Multicast Configuration > MLD Proxy**.

Step 2 Enter the following fields:

- MLD Multicast Routing—Select to enable IPv6 Multicast routing.
- Downstream Protection—Select to discard downstream packets not required for the device.
- Source Specific Multicast—Select to enable delivering Multicast packets originating from a specific source address defined in the next field.
- SSM IPv6 Access List—Define the list containing source addresses from which to deliver Multicast packets:
  - Default list—Defines the SSM range access list to FF3E::/32.
  - User-defined access list—Select the standard IPv6 access list name defining the SSM range. These access lists are defined in IPv6 Access Lists, on page 240.

Step 3 Click **Apply**. The Running Configuration file is updated.

Step 4 To add protection to a VLAN, click **Add** and enter the following fields:

- Upstream Interface—Select the outgoing interface.
- Downstream Interface—Select the incoming interface.
- Downstream Protection—Select one of the following options:
  - Use global—Use the status set in the global block.
  - Disable—This enables forwarding of IPv6 Multicast traffic from downstream interfaces.
  - Enable—This disables forwarding from downstream interfaces.

Step 5 Click **Apply**. The Running Configuration file is updated.

The following fields are displayed for each IPv6 Multicast route:

- Source Address—Unicast source IPv4 address.
- Group Address—Multicast destination IPv4 address.
- Incoming Interface—Expected interface for a Multicast packet from the source. If the packet isn't received on this interface, it's discarded.
- Outgoing Interfaces—Interfaces through which packets will be forwarded.
- Uptime—Length of time in hours, minutes, and seconds that the entry has been in the IP Multicast routing table.
- Expiry Time—Length of time in hours, minutes, and seconds until the entry is removed from the IP Multicast routing table.

IGMP/MLD Snooping IP Multicast Group

The IGMP/MLD Snooping IP Multicast Group page displays the IPv4 and IPv6 group addresses learned from IGMP/MLD messages.

There might be a difference between information on this page and information on the MAC Group Address page. For example, assume that the system filters according to MAC-based groups and a port requested to join the following Multicast groups 224.1.1.1 and 225.1.1.1. Both are mapped to the same MAC Multicast address 01:00:5e:01:01:01. In this case, there's a single entry in the MAC Multicast page, but two entries on this page.

To query for an IP Multicast group, complete the following steps:

Procedure

Step 1 Click **Multicast** > **IGMP/MLD Snooping IP Multicast Group**.

Step 2 Set the type of snooping group for which to search: IGMP or MLD.

Step 3 Enter some or all of following query filter criteria:

- Group Address equals to—Defines the Multicast group MAC address or IP address to query.
- Source Address equals to—Defines the sender address to query.
- VLAN ID equals to—Defines the VLAN ID to query.

Step 4 Click **Go**. The following fields are displayed for each Multicast group:

- VLAN—The VLAN ID.
- Group Address—The Multicast group MAC address or IP address.
- Source Address—The sender address for all of the specified group ports.

- Included Ports—The list of destination ports for the Multicast stream.
- Excluded Ports—The list of ports not included in the group.
- Compatibility Mode—The oldest IGMP/MLD version of registration from the hosts the device receives on the IP group address.

Multicast Router Port

A Multicast router (Mrouter) port is a port that connects to a Multicast router. The device includes one or more Multicast router ports numbers when it forwards the Multicast streams and IGMP/MLD registration messages. This is required so that the Multicast routers can, forward the Multicast streams and propagate the registration messages to other subnets.

To statically configure or to view the dynamically detected ports connected to the Multicast router, follow these steps:

Procedure

Step 1 Click **Multicast** > **Multicast Router Port**.

Step 2 Enter some or all of following query filter criteria:

- VLAN ID equals to—Select the VLAN ID for the router ports that are described.
- IP Version equals to—Select the IP version that the Multicast router supports.
- Interface Type equals to—Select whether to display ports or LAGs.

Step 3 Click **Go**. The interfaces matching the query criteria are displayed.

Step 4 For each port or LAG, select its association type. The options are as follows:

- Static—The port is statically configured as a Multicast router port.
- Dynamic—(Display only) The port is dynamically configured as a Multicast router port by a MLD/IGMP query. To enable the dynamic learning of Multicast router ports, go to IGMP/MLD Snooping IP Multicast Group, on page 196.
- Forbidden—This port isn't to be configured as a Multicast router port, even if IGMP or MLD queries are received on this port. If Forbidden is enabled on a port, the MRouter isn't learned on this port (i.e. MRouter Ports Auto-Learn isn't enabled on this port).
- None—The port isn't currently a Multicast router port.

Step 5 Click **Apply** to update the device.

Forward All

When Bridge Multicast Filtering is enabled, registered Multicast packets are forwarded to ports based on IGMP and MLD snooping. If Bridge Multicast Filtering is disabled, all Multicast packets are flooded to the corresponding VLAN.

The Forward All page configures the ports and/or LAGs that receive Multicast streams from a specific VLAN. This feature requires that the Bridge Multicast filtering is enabled in Multicast Properties, on page 183. If it is disabled, then all Multicast traffic is flooded to the ports on the device. You can statically (manually) configure a port to Forward All, if the devices connecting to the port don't support IGMP and/or MLD. Multicast packets, excluding IGMP and MLD messages, are always forwarded to ports that are defined as Forward All. The configuration affects only the ports that are members of the selected VLAN.

To define Forward All Multicast, complete the following steps:

Procedure

Step 1 Click **Multicast** > **Forward All**.

Step 2 Define the following:

- VLAN ID equals to—The VLAN ID the ports/LAGs are to be displayed.
- Interface Type equals to—Define whether to display ports or LAGs.

Step 3 Click **Go**. The status of all ports/LAGs are displayed.

Step 4 Select the port/LAG that is to be defined as Forward All by using the following methods:

- Static—The port receives all Multicast streams.
- Forbidden—Ports can't receive any Multicast streams, even if IGMP/MLD snooping designated the port to join a Multicast group.
- None—The port isn't currently a Forward All port.

Step 5 Click **Apply**. The Running Configuration file is updated.

Unregistered Multicast

This feature is used to ensure that the customer receives only the Multicast groups requested (registered).

Unregistered Multicast frames are forwarded to all ports on the VLAN. You can select a port to filter unregistered Multicast streams. The configuration is valid for any VLAN of which the port is a member.

To define unregistered Multicast settings, follow these steps:

Procedure

Step 1 Click **Multicast** > **Unregistered Multicast**.

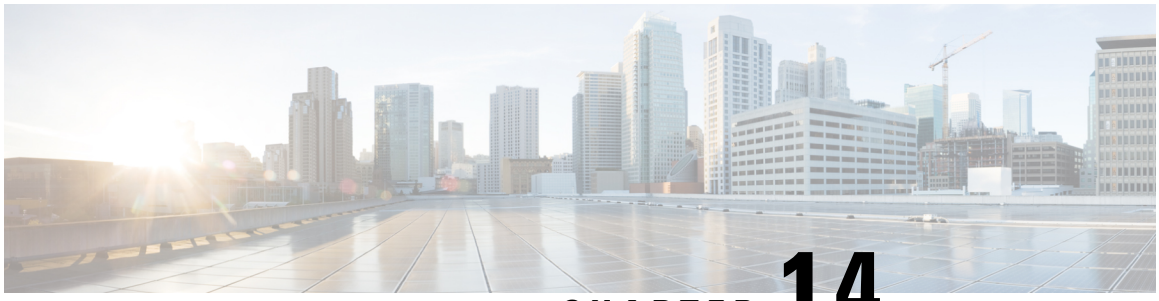
Step 2 Select the Interface Type equals to— To view either ports or LAGs.

Step 3 Click **Go**.

Step 4 Define the following:

- Port/LAG—Displays the port or LAG ID.
- Displays the forwarding status of the selected interface. The possible values are:
  - Forwarding—Enables forwarding of unregistered Multicast frames to the selected interface.
  - Filtering—Enables filtering (rejecting) of unregistered Multicast frames to the selected interface.

Step 5 Click **Apply**. The settings are saved, and the Running Configuration file is updated.



CHAPTER 14

IPv4 Configuration

This chapter contains the following sections:

- IPv4 Interface, on page 201
- IPv4 Static Routes, on page 204
- IPv4 Forwarding Table, on page 205
- RIPv2, on page 206
- Access List, on page 210
- ARP, on page 212
- ARP Proxy, on page 213
- UDP Relay/IP Helper, on page 213
- DHCP Snooping/Relay, on page 214
- DHCP Server, on page 220

IPv4 Interface

IPv4 interface addresses can be configured manually by the user, or automatically configured by a DHCP server. This section provides information for defining the device IPv4 addresses, either manually or by making the device a DHCP client. The IPv4 Interface page is used to configure IP addresses for device management. This IP address can be configured on a port, a LAG, VLAN, loopback interface or out-of-band interface. You can configure multiple IP addresses (interfaces) on the device. It then supports traffic routing between these various interfaces and also to remote networks. By default and typically, the routing functionality is performed by the hardware. If hardware resources are exhausted or there's a routing table overflow in the hardware, IP routing is performed by the software.

Note The device software consumes one VLAN ID (VID) for every IP address configured on a port or LAG. The device takes the first VID that isn't used starting from 4094.

To configure the IPv4 addresses, follow these steps:

Procedure

Step 1 Click **IPv4 Configuration** > **IPv4 Interface.**

Enter the following fields:

- IPv4 Routing—Check the Enable box to enable IPv4 routing (enabled by default).

Step 2 Click **Apply**. The parameter is saved to the Running Configuration file.

The following fields are displayed in the IPv4 Interface Table:

- Interface—Interface for which the IP address is defined. This can also be the out-of-band port.
- IP Address Type—The available options are:
  - DHCP—Received from DHCP server
  - Static—Entered manually. Static interfaces are non-DHCP interfaces that created by the user.
  - Default—The default address that exists on the device by default, before any configurations have been made.
- IP Address—Configured IP address for the interface.
- Mask—Configured IP address mask.
- Status—Results of the IP address duplication check.
  - Tentative—There's no final result for the IP address duplication check.
  - Valid—The IP address collision check was completed, and no IP address collision was detected.
  - Valid-Duplicated—The IP address duplication check was completed, and a duplicate IP address was detected.
  - Duplicated—A duplicated IP address was detected for the default IP address.
  - Delayed—The assignment of the IP address is delayed for 60 second if DHCP Client is enabled on startup in order to give time to discover DHCP address.
  - Not Received—Relevant for DHCP Address When a DCHP Client starts a discovery process, it assigns a dummy IP address 0.0.0.0 before the real address is obtained. This dummy address has the status of "Not Received".

Step 3 Click **Add.**

Step 4 Select the Interface: Select the port, LAG, VLAN or loopback as the interface associated with this IP configuration, and select an interface from the list. select an interface from the associated list.

Step 5 Select the IP Address Type: Select one of the following options:

- Dynamic IP Address—Receive the IP address from a DHCP server.
- Static IP Address—Enter the IP address, and enter the Mask field:
  - Network Mask—IP mask for this address
  - Prefix Length—Length of the IPv4 prefix
- Renew IP Address Now—Check **Enable** to enable.
- Auto Configuration via DHCP—Display the status (Disabled or Enabled).

Step 6 Click **Apply**. The IPv4 address settings are written to the Running Configuration file.

Caution

When the system is in one of the stacking modes with a standby active unit present, Cisco recommends configuring the IP address as a static address to prevent disconnecting from the network during a active stacking unit switchover. This is because when the standby active unit takes control of the stack, when using DHCP, it might receive a different IP address than the one that was received by the stack's original active-enabled unit.

Configure the Out-of-Band Interface

Out-of-band management allows the network operator to establish trust boundaries in accessing the management function to apply it to network resources. This section describes how to configure the IPv4 address on the Out-of-Band (OOB) interface.

Procedure

Step 1 Log in to the web-based utility of the switch then choose **IPv4 Configuration > IPv4 Interface**.

The IPv4 Interface Table on the IPv4 Interface page contains the following information:

- Interface — The Unit or interface for which the IP address is defined. This can also be a loopback interface.
- IP Address Type — The available options are:
  - DHCP — Received from Dynamic Host Configuration Protocol (DHCP) server.
  - Static — Entered manually. Static interfaces are non-DHCP interfaces that are created by the user.
  - Default — The default address that exists on the device by default, before any configurations have been made.
- IP Address — Configured IP address for the interface.
- Mask — Configured IP address mask.
- Status — Results of the IP address duplication check.
  - Tentative — There is no final result for the IP address duplication check.
  - Valid — The IP address collision check was completed, and no IP address collision was detected.
  - Valid-Duplicated — The IP address duplication check was completed, and a duplicate IP address was detected.
  - Duplicated — A duplicated IP address was detected for the default IP address.
  - Delayed — The assignment of the IP address is delayed for 60 seconds if DHCP Client is enabled on startup in order to give time to discover DHCP address.
  - Not Received — Relevant only for DHCP Address. When a DHCP Client starts a discovery process, it assigns a dummy IP address 0.0.0.0 before the real address is obtained. This dummy address has the status of Not Received.

Step 2 Click **Add** to manually assign a static IP address.

Step 3 From the Interface area, select **Out of Band**.

Step 4 Select **Static IP Address** from the IP Address Type area.

Step 5 Enter the IP address of the OOB interface in the *IP Address* field.

Step 6 Click a radio button from the Mask area then enter the corresponding subnet mask. The options are:

- Network Mask — IP mask for this address.
- Prefix Length — Length of the IPv4 prefix.

Step 7 Click **Apply** then click **Close**.

Your session will be automatically closed and connection to the switch will be lost as it will apply the new management IP address on the OOB port.

You should now have successfully configured the IPv4 management interface addresses on your switch.

IPv4 Static Routes

This page enables configuring and viewing IPv4 static routes on the device. When routing traffic, the next hop is decided on according to the longest prefix match (LPM algorithm). A destination IPv4 address may match multiple routes in the IPv4 Static Route Table. The device uses the matched route with the highest subnet mask, that is, the longest prefix match. If more than one default gateway is defined with the same metric value, the lowest IPv4 address from among all the configured default gateways is used.

To define an IP static route, follow these steps:

Procedure

Step 1 Click **IPv4 Configuration** > **IPv4 Static Routes**.

The IPv4 Static Routes Table is displayed. The following fields are displayed for each entry:

- Destination IP Prefix-Destination IP address prefix.
- Prefix Length- IP route prefix for the destination IP.
- Route Type-Whether the route is a reject or remote route.
- Next Hop Router IP Address-The next hop IP address or IP alias on the route.
- Metric-Cost of this hop (a lower value is preferred).
- Outgoing Interface-Outgoing interface for this route.

Step 2 Click **Add.**

Step 3 Enter values for the following fields:

- Destination IP Prefix-Enter the destination IP address prefix.
- Mask-Select and enter:
  - Network Mask-IP route prefix for the destination IP, in the format of a mask (number of bits in of route network address)

- Prefix Length-IP route prefix for the destination IP in IP address format

- Route Type-Select the route type.
  - Reject-Rejects the route and stops routing to the destination network via all gateways This ensures that if a frame arrives with the destination IP of this route, it's dropped. Selecting this value disables the following controls: Next Hop IP Address, Metric, and IP SLA Track.
  - Remote-Indicates that the route is a remote path

- Next Hop Router IP Address-Enter the next hop IP address or IP alias on the route.

  Note
  You can't configure a static route through a directly connected IP subnet where the device gets its IP address from a DHCP server.

- Metric select one of the following:
  - Use Default - select this to use the default metric.
  - User Defined - Enter the administrative distance to the next hop. The range is 1–255.

Step 4 Click **Apply**. The IP Static route is saved to the Running Configuration file.

IPv4 Forwarding Table

To view the IPv4 Forwarding Table, follow these steps:

Procedure

Step 1 Click **IPv4 Configuration** > **IPv4 Forwarding Table**.

The IPv4 Forwarding Table is displayed. The following fields are displayed for each entry:

- Destination IP Prefix—Destination IP address prefix.
- Prefix Length— IP route prefix for the length of the destination IP.
- Route Type—Whether the route is a local, reject or remote route.
- Next Hop Router IP Address—The next hop IP address.
- Route Owner—This can be one of the following options:
  - Default—Route was configured by default system configuration.
  - Static—Route was manually created.
  - Dynamic—Route was created by an IP routing protocol.
  - DHCP—Route was received from a DHCP server.

- Directly Connected—Route is a subnet to which the device is connected.
- Rejected—Route was rejected.

- Metric—Cost of this hop (a lower value is preferred).
- Administrative Distance—The administrative distance to the next hop (a lower value is preferred). This isn't relevant for static routes.
- Outgoing Interface—Outgoing interface for this route.

Step 2 Click the **Refresh** icon to refresh the data.

RIPv2

This section describes the Routing Information Protocol (RIP) version 2 feature.

Note This feature is only supported on firmware 3.1 and beyond.

Routing Information Protocol (RIP) is an implementation of a distance-vector protocol for local and wide-area networks. It classifies routers as either active or passive (silent). Active routers advertise their routes to others; passive routers listen and update their routes based on advertisements, but do not advertise. Typically, routers run RIP in active mode, while hosts usepassive mode.

The default gateway is a static route and it is advertised by RIP in the same way as all other static routers, if it is enabled by configuration. When IP Routing is enabled, RIP works fully. When IP Routing is disabled, RIP works in the passive mode, meaning that it only learns routes from the received RIP messages and does not send them.

Note To enable IP Routing, go to the IPv4 Interface page. The device supports RIP version 2, which is based on the following standards:

- RFC2453 RIP Version 2, November 1998
- RFC2082 RIP-2 MD5 Authentication, January 1997
- RFC1724 RIP Version 2 MIB Extension

Received RIPv1 packets are dropped.

Enabling RIP

- RIP must be enabled globally and per interface.
- RIP can only be configured if it is enabled.
- Disabling RIP globally deletes the RIP configuration on the system.

- Disabling RIP on an interface deletes the RIP configuration on the specified interface.
- If IP Routing is disabled, RIP messages are not sent, although when RIP messages are received, they are used to update the routing table information.



Note RIP can only be defined on manually-configured IP interfaces, meaning that RIP cannot be defined on an interface whose IP address was received from a DHCP server or whose IP address is the default IP address.

RIPv2 Properties

To enable or disable RIPv2 on the device, follow these steps:

Procedure

Step 1 Click **IPv4 Configuration** > **RIPv2** > **RIPv2 Properties**.

Step 2 Select the following options as required:

- RIP—The following options are available:
  - Enable—Enable RIP.
  - Disable—Disable RIP. Disabling RIP deletes the RIP configuration on the system.
  - Shutdown—Set the RIP global state to shutdown.
- RIP Advertisement—Select to enable sending routing updates on all RIP IP interfaces.
- Default Route Advertisement—Select to enable sending the default route to the RIP domain. This route will serve as the default router.
- Default Metric—Enter the value of the default metric.

Step 3 Redistribute Static Route—Select to enable manually-defined (remote) routes.

Step 4 If Redistribute Static Route is enabled, select an option for the Redistribute Static Metric field. The following options are available:

- Default Metric—Causes RIP to use the default metric value for the propagated static route configuration.
- Transparent—Causes RIP to use the routing table metric as the RIP metric fo
  - If the metric value of a static route is equal to or less than 15, this value is used in the RIP protocol when advertising this static route.
  - If the metric value of a static route is greater than 15, the static route is not advertised to other routers using RIP.
- User Defined Metric—Enter the value of the metric.

Step 5 Redistribute Connected Route—Select to enable RIP routes that correspond to defined IP interfaces on which RIP is not enabled (defined locally).

Step 6 If Redistribute Connected Route is enabled, select an option for the Redistribute Connected Metric field. The following options are available:

- Default Metric—Causes RIP to use the default metric value for the propagated static route configuration.
- Transparent—Causes RIP to use the routing table metric as the RIP metric for the propagated static route configuration. This results in the following behavior:
  - If the metric value of a static route is equal to or less than 15, this value is used in the RIP protocol when advertising this static route.
  - If the metric value of a static route is greater than 15, the static route is not advertised to other routers using RIP.
- User Defined Metric—Enter the value of the metric.

Step 7 Click **Apply**. The settings are written to the Running Configuration file.

RIPv2 Settings

To configure RIP on an IP interface, complete the following steps:

Procedure

Step 1 Click **IPv4 Configuration** > **RIPv2** > **RIPv2 Settings**.

Step 2 RIP parameters are displayed per IP interface. To add a new IP interface, click **Add** and enter the following fields:

- IP Address—Select an IP interface defined on the Layer 2 interface.
- Shutdown—Keep RIP configuration on the interface, but set the interface to inactive.
- Passive—Specifies whether sending RIP route update messages is allowed on the specified IP interface. If this field isn't enabled, RIP updates aren't sent (passive).
- Offset—Specifies the metric number of the specified IP interface. This reflects the additional cost of using this interface, based on the speed of the interface.
- Default Route Advertisement—This option is defined globally in the RIPv2 Properties, on page 207 page. You can use the global definition or define this field for the specific interface. The following options are available:
  - Global—Use the global settings defined in the RIPv2 Properties. Screen
  - Disable—On this RIP interface, don't advertise the default route.
  - Enable—Advertise the default route on this RIP interface.
- Default Route Advertisement Metric—Enter the metric for the default route for this interface.
- Authentication Mode—RIP authentication state (enable/disable) on a specified IP interface. The following options are available:

- None—There's no authentication performed.
- Text—The key password entered below is used for authentication.
- MD5—The MD5 digest of the key chain selected below is used for authentication.

- Key Password—If Text was selected as the authentication type, enter the password to be used.
- Key Chain—If MD5 was selected as the authentication mode, enter the key chain to be digested. This key chain is created as described in the section.
- Distribute-list In—Select to configure filtering on RIP incoming routes for one or more specified IP addresses in the Access List Name. If this field is enabled, select the Access List Name below.
- Access List Name—Select the Access List name (which includes a list of IP addresses) of RIP incoming routes filtering for a specified IP interface.
- Distribute-list Out—Select to configure filtering on RIP outgoing routes for one or more specified IP addresses in the Access List Name. If this field is enabled, select the Access List Name below.
- Access List Name—Select the Access List name (which includes a list of IP addresses) of RIP outgoing routes filtering for a specified IP interface.

Step 3 Click **Apply**. The settings are written to the Running Configuration file.

RIPv2 Statistics

To view the RIP statistical counters for each IP address, complete the following steps:

Procedure

Step 1 Click **IPv4 Configuration** > **RIPv2** > **RIPv2 Statistics**.

The following fields are displayed:

- IP Interface—IP interface defined on the Layer 2 interface.
- Bad Packets Received—Specifies the number of bad packets identified by RIP on the IP interface.
- Bad Routes Received—Specifies the number of bad routes received and identified by RIP on the IP interface. Bad routes mean that the route parameters are incorrect. For example, the IP destination is a Broadcast address, or the metric is 0 or greater than 16.
- Update Sent—Specifies the number of packets sent by RIP on the IP interface.

Step 2 To clear all interface counters, click **Clear All Interface Counters**.

RIPv2 Peer Router Database

To view RIP Peer Router Database, follow these steps:

Procedure

Step 1 Click **IPv4 Configuration** > **RIPv2** > **RIPv2 Peer Router Database**.

The following fields are displayed for the peer router database:

- **Router IP Address**—IP interface defined on the Layer 2 interface.
- **Bad Packets Received**—Specifies the number of bad packets identified by RIP on the IP interface.
- **Bad Routes Received**—Specifies the number of bad routes received and identified by RIP on the IP interface. Bad routes mean that the route parameters are incorrect. For example, the IP destination is a Broadcast, or the metric is 0 or greater than 16.
- **Last Updated**—Indicates the last time RIP received RIP routes from the remote IP address.

Step 2 To clear all counters, click **Clear All Interface Counters**.

Access List

Access lists consists of permit and/or deny statements that filter traffic on a device. These statements are executed in a top down fashion. As traffic encounters the access list, the access list is parsed top to bottom, looking for a match. The first match encountered will determine if the traffic is permitted or denied. Therefore, the order of your access list statements is extremely important. Access list should be built from most specific to least specific. This will keep unintentional matching to a minimum. If no match is found, there is an implicit "deny everything" at the end of all access list statements.

Access lists are an integral part of working with switches, and they are vital to security.

Access List Settings

To set the global configuration of an access list, follow these steps:

Procedure

Step 1 Click **IPv4 Configuration** > **Access List** > **Access List Settings**.

Step 2 To add a new Access List, click **Add** to open the Add Access List page and enter the following fields:

- Name—Define a name for the access list.
- Source IPv4 Address—Enter the source IPv4 address. The following options are available:
  - Any—All IP addresses are included.

- User defined—Enter an IP address.

- Source IPv4 Mask—Enter the source IPv4 address mask type and value. The following options are available:
  - Network mask—Enter the network mask.
  - Prefix length—Enter the prefix length.
- Action—Select an action for the access list. The following options are available:
  - Permit—Permit entry of packets from one or more IP addresses in the access list.
  - Deny—Reject entry of packets from one or more IP addresses in the access list.

Step 3 Click **Apply**. The settings are written to the Running Configuration file.

Source IPv4 Address List

To populate an access list with IP addresses, complete the following:

Procedure

Step 1 Click **IPv4 Configuration** > **Access List** > **Source IPv4 Address List**.

Step 2 To modify the parameters of an access list, click **Add** and modify any of the following fields:

- Access List Name—Name of the access list.
- Source IPv4 Address—Source IPv4 address. The following options are available:
  - Any—All IP addresses are included.
  - User defined—Enter an IP address.
- Source IPv4 Mask—Source IPv4 address mask type and value. The following options are available:
  - Network mask—Enter the network mask (for example 255.255.0.0).
  - Prefix length—Enter the prefix length.
- Action—Action for the access list. The following options are available:
  - Permit—Permit entry of packets from one or more IP addresses in the access list.
  - Deny—Reject entry of packets from one or more IP addresses in the access list.

Step 3 Click **Apply**. The settings are written to the Running Configuration file.

ARP

The device maintains an ARP (Address Resolution Protocol) table for all known devices that reside in the IP subnets directly connected to it. A directly connected IP subnet is the subnet to which an IPv4 interface of the device is connected. When the device is required to send/route a packet to a local device, it searches the ARP table to obtain the MAC address of the device. The ARP table contains both static and dynamic addresses. Static addresses are manually configured and don't age out. The device creates dynamic addresses from the ARP packets it receives. Dynamic addresses age out after a configured time.



Note The mapping information is used for routing and to forward generated traffic.

To define the ARP tables, complete the following steps:

Procedure

Step 1 Click **IPv4 Configuration** > **ARP**.

Step 2 Enter the parameters.

- ARP Entry Age Out—Enter the number of seconds that dynamic addresses can remain in the ARP table. A dynamic address age out after the time it's in the table exceeds the ARP Entry Age Out time. When a dynamic address ages out, it's deleted from the table, and only returns when it's relearned.
- Clear ARP Table Entries—Select the type of ARP entries to be cleared from the system.
  - All—Deletes all of the static and dynamic addresses immediately
  - Dynamic—Deletes all of the dynamic addresses immediately
  - Static—Deletes all of the static addresses immediately
  - Normal Age Out—Deletes dynamic addresses based on the configured ARP Entry Age Out time.

Step 3 Click **Apply.** The ARP global settings are written to the Running Configuration file.

The ARP table displays the following fields:

- Interface—The IPv4 Interface of the directly connected IP subnet where the IP device resides.
- IP Address—The IP address of the IP device.
- MAC Address—The MAC address of the IP device.
- Status—Whether the entry was manually entered or dynamically learned.

Step 4 Click **Add**.

Step 5 Enter the parameters:

- IP Version—The IP address format supported by the host. Only IPv4 is supported.

- Interface—An IPv4 interface can be configured on a port, LAG, or VLAN. Select the desired interface from the list of configured IPv4 interfaces on the device.
- IP Address—Enter the IP address of the local device.
- MAC Address—Enter the MAC address of the local device.

Step 6 Click **Apply**. The ARP entry is saved to the Running Configuration file.

ARP Proxy

The Proxy ARP technique is used by the device on a given IP subnet to answer ARP queries for a network address that isn't on that network.



Note The ARP proxy feature is only available when the device is in L3 mode.

The ARP Proxy is aware of the destination of traffic, and offers another MAC address in reply. Serving as an ARP Proxy for another host effectively directs LAN traffic destination to the host. The captured traffic is then typically routed by the Proxy to the intended destination by using another interface, or by using a tunnel. The process in which an ARP-query-request for a different IP address, for proxy purposes, results in the node responding with its own MAC address is sometimes referred to as publishing.

To enable ARP Proxy on all IP interfaces, complete the following steps:

Procedure

Step 1 Click **IPv4 Configuration** > **ARP Proxy**.

Step 2 Select **ARP Proxy** to enable the device to respond to ARP requests for remotely-located nodes with the device MAC address.

Step 3 Click **Apply**. The ARP proxy is enabled, and the Running Configuration file is updated.

UDP Relay/IP Helper

Switches don't typically route IP Broadcast packets between IP subnets. However, this feature enables the device to relay specific UDP Broadcast packets, received from its IPv4 interfaces, to specific destination IP addresses.

To configure the relaying of UDP packets received from a specific IPv4 interface with a specific destination UDP port, add a UDP Relay:

Procedure

Step 1 Click **IPv4 Configuration** > **UDP Relay/IP Helper**.

Step 2 Click **Add.**

Step 3 Select the Source IP Interface to where the device is to relay UDP Broadcast packets based on a configured UDP destination port. The interface must be one of the IPv4 interfaces configured on the device.

Step 4 Enter the UDP Destination Port number for the packets that the device is to relay. Select a well-known port from the drop-down list, or click the port radio button to enter the number manually.

Step 5 Enter the Destination IP Address that receives the UDP packet relays. If this field is 0.0.0.0, UDP packets are discarded. If this field is 255.255.255.255, UDP packets are flooded to all IP interfaces.

Step 6 Click **Apply**. The UDP relay settings are written to the Running Configuration file.

DHCP Snooping/Relay

This section covers Dynamic Host Configuration Protocol (DHCP) Snooping/Relay. A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently. By contrast, relay agents receive DHCP messages and then generate a new DHCP message to send on another interface.

DHCP snooping is a layer 2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. The fundamental use case for DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients.

Properties

DHCP Relay transfers DHCP packets to the DHCP server.

To set the DHCP Snooping/Relay properties, complete the following steps:

Procedure

Step 1 Click **IPv4 Configuration** > **DHCP Snooping/Relay** > **Properties**.

Step 2 Configure the following fields:

- DHCP Relay—Select to enable DHCP Relay
- DHCP Snooping Status—Select to enable DHCP Snooping.
- Option 82 Pass Through—Select to leave foreign Option 82 information when forwarding packets.
- Verify MAC Address—Select to verify that the source MAC address of the Layer 2 header matches the client hardware address as appears in the DHCP Header (part of the payload) on DHCP untrusted ports.

- Backup Database—Select to back up the DHCP Snooping Binding database on the device's flash memory.

Step 3 Click **Apply**. The settings are written to the Running Configuration file.

Step 4 To define a DHCP server, click **Add**. The Add DHCP Server dialog appears, with the IP version indicated.

Step 5 Enter the IP address of the DHCP server and click **Apply**. The settings are written to the Running Configuration file.

Option 82 Settings

Option 82 (DHCP Relay Agent Information Option) passes port and agent information to a central DHCP server, indicating where an assigned IP address physically connects to the network. The main goal of option 82 is to help to the DHCP server select the best IP subnet (network pool) from which to obtain an IP address.

Option 82, when enabled, applies to DHCP Relay interface with IP address and DHCP Snooping. Even if Option 82 isn't enabled, and if DCHP relay is enabled on VLAN without an IP address, option 82 information will be inserted to DHCP packets received on this VLAN.

To configure the status on the device and the format of the Option 82 data within the DHCP message, follow these steps:

Procedure

Step 1 Click **IPv4 Configuration > DHCP Snooping/Relay > Option 82 Settings**.

Enter the following fields:

- Option 82 Insertion—Check Enable to insert Option 82 information into packets.
- Numeric Token Format—Select Hexadecimal or Ascii as needed. This parameter defines the format to use for the following tokens:
  - $int-ifindex$
  - $int-portid$
  - $switch-moduleid$
  - $vlan-id$

  For example, the $vlan-id$ token, where VLAN ID is 35. VLAN ID 35 can be sent either as Hexa byte of 0x23 or ASCII representation of value of 0x3335. See the full information on the various tokens in the following table.

Step 2 Enter the Circuit-ID Template. Select **Use Default** to use the default Circuit-ID. Select **User Defined** to configure the Circuit-ID. Use the text box to enter the Circuit-ID template. The template is a string of free text and pre-defined tokens (see table below). You can enter tokens manually, or use the drop-down to select a token from the list of available tokens and add it to the Circuit-ID text by clicking the arrow button. Use the Preview button to view actual Sub option byte content and text representation of the selected sub-option.

Step 3 Enter the Remote-ID Template in the same way as the Circuit-ID Template, using the related text box and drop-down list.

Note

The **Total Sub-Option Payload** shows the dynamically updated number of reserved byte count of the payload of both sub-options. The payload must not exceed 247. Byte count is based on the reserved length of the tokens included in the sub-option, plus the number of free text chars used in the sub-option.

Step 4 Click **Apply**. The settings are written to the Running Configuration file.

These are the tokens that are available from the drop-down box.

Option	Description	Reserved bytes	Bytes used in Hex format	Byt ASC
$int-ifindex$	The ifIndex of the interface on which the DHCP client request was received. Value is taken from the ifIndex field of the ifTable MIB entry	4	2	4
$int-portid$	The interface number relative to the specific unit (standalone or stacking unit). For physical interfaces this value begins with 1 for the 1st port on a specific unit, 2 for the 2nd port on that unit, until N for last port on that unit. For LAG interfaces the value is determined globally (and not based on specific unit), according to the LAG ID. For example, 1,2,3….	2	1	2
$int-name$	The full name of the interface, upon which the DHCP client request was received. The name is based on the interface full name format as used by CLI when configuring or displaying information for this interface	32	NA	Act for repr the nan lim byt
$int-abrvname$	The abbreviated name of the interface, upon which the DHCP client request was received. This parameter is based on the abbreviated interface name format as used by CLI when configuring or displaying information for this interface.	8	NA	
$int-desc-16$	Up to 16 (first) bytes of the interface description- for the interface, upon which the DHCP client packet was received. The value for this variable is taken from the description added by the user to the interface using the interface level "description" command. Max number of bytes to use is 16 (first bytes)- even if description is longer than 16 bytes. For interfaces without a user-defined description- the interface abbreviated interface name format is used.	16	NA	Act for repr the des the rese

Option	Description	Reserved bytes	Bytes used in Hex format
$int-desc-32$	Up to 32 (first) bytes of the interface description - for the interface, upon which the DHCP client packet was received. The value for this variable is taken from the description added by the user to the interface using the interface level "description" command. Max number of bytes to use is 32 (1st bytes) - even if description is longer than 32 bytes. For interfaces without user-defined description - the interface abbreviated interface name format is used.	32	NA
$int-desc-64$	The full interface description (up to 64 bytes) - for the interface, upon which the DHCP client packet was received. The value for this variable is taken from the description added by the user to the interface using the interface level "description" command. For interfaces without user-defined description - the interface abbreviated interface name format is used.	64	NA
$int-mac$	The MAC address of the physical interface upon which the DHCP client request was received. The format of this field is always HEX format, with no delimiter (for example, 000000112205).	6	6
$switch-mac$	The base MAC address of the device inserting the option 82 (the relay agent). The format of this field is always HEX format, with no delimiter (for example, 000000112200).	6	6
$switch-hostname-16$	Up to the first 16 bytes of the device hostname.	16	NA
$switch-hostname-32$	Up to the first 32 bytes of the device hostname.	32	NA
$switch-hostname-58$	The full hostname of the device.	58	NA
$switch-module-id$	The unit ID of the unit upon which the DHCP client request was received. In standalone systems ID is always equal 1.	2	1
$vlan-id$	The VLAN ID of the VLAN upon the DHCP client request was received. Values 1-4094	4	2

Option	Description	Reserved bytes	Bytes used in Hex format	Byt ASC
$vlan-name-16$	Up to the first 16 bytes of the VLAN name, for the VLAN upon which the DHCP client request was received. If a name isn't configure for the specified VLAN, the value is taken from the relevant VLAN ifDescr MIB field of ifTable MIB entry.	16	NA	Act for repr the (up rese
$vlan-name-32$	The full VLAN name of the VLAN upon the DHCP client request was received. If a name is configure for the specified VLAN, the value is taken from the relevant ifDescr MIB field of ifTable MIB entry.	32	NA	

Note The total reserved byte count of the payload of both sub-options must not exceed 247. The byte count isn't updated dynamically and shown at the bottom of the screen. Byte count is based on the reserved length (see above) of the tokens included in the sub-option, plus the number of free text chars used in the sub-option.

Interface Settings

DHCP Relay and Snooping can be enabled on any interface or VLAN. For DHCP relay to be functional, an IP address must be configured on the VLAN or interface.

DHCPv4 Relay Overview

DHCP Relay relays DHCP packets to the DHCP server. The device can relay DHCP messages received from VLANs that do not have IP addresses. Whenever DHCP Relay is enabled on a VLAN without an IP address, Option 82 is inserted automatically. This insertion is in the specific VLAN and does not influence the global administration state of Option 82 insertion.

DHCPv4 Snooping Overview

DHCP snooping provides a security mechanism to prevent receiving false DHCP response packets and to log DHCP addresses. It does this by treating ports on the device as either trusted or untrusted. A trusted port is a port that is connected to a DHCP server and is allowed to assign DHCP addresses. DHCP messages received on trusted ports are allowed to pass through the device. An untrusted port is a port that is not allowed to assign DHCP addresses. By default, all ports are considered untrusted until you declare them trusted (in the Interface Settings page).

To enable DHCP Snooping/Relay on specific interfaces, follow these steps:

Procedure

Step 1 Click **IPv4 Configuration > DHCP Snooping/ Relay > Interface Settings.**

Step 2 To enable DHCP Relay or DHCP Snooping on an interface, click **ADD**.

Step 3 Select the interface and the feature to be enabled: **DHCP Relay** or **DHCP Snooping** or both to enable.

Note
The DHCP snooping setting is available only if there is an IP address configured on the selected interface.

Step 4 Click **Apply**. The settings are written to the Running Configuration file.

DHCP Snooping Trusted Interfaces

Packets from untrusted ports/LAGs are checked against the DHCP Snooping Binding database (See DHCP Snooping Binding Database, on page 219). By default, interfaces are untrusted. To designate an interface as trusted, follow these steps:

Procedure

Step 1 Click **IPv4 Configuration** > **DHCP Snooping/Relay** > **DHCP Snooping Trusted Interfaces.**
Step 2 Select the interface and click **Edit**.
Step 3 Select **Trusted Interface** (**Yes** for trusted or **No** for untrusted).
Step 4 Click **Apply** to save the settings to the Running Configuration file.

DHCP Snooping Binding Database

Note the following points about maintenance of the DHCP Snooping Binding database:

- The device doesn't update the DHCP Snooping Binding database when a station moves toanother interface.
- If a port is down, the entries for that port aren't deleted.
- When DHCP Snooping is disabled for a VLAN, the binding entries that collected for that VLAN are removed.
- If the database is full, DHCP Snooping continue to forward packets but new entries aren't created. Note that if the IP source guard and/or ARP inspection features are active, the clients that aren't written in the DHCP Snooping Binding database aren't been able to connect to the network.

To add entries to the DHCP Snooping Binding database, follow these steps:

Procedure

Step 1 Click **IPv4 Configuration > DHCP Snooping /Relay > DHCP Snooping Binding Database**.

The fields in the DHCP Snooping Binding Database are displayed for the IP Source Guard:

- Status
  - Active—IP Source Guard is active on the device.
  - Inactive—IP Source Guard isn't active on the device.

- Reason
  - No Problem
  - No Resource
  - No Snoop VLAN
  - Trust Port

Step 2 To add an entry, click **Add**. The supported address type is IPv4.

Step 3 Enter the fields:

- VLAN ID—VLAN on which packet is expected.
- MAC Address—MAC address of packet.
- IP Address—IP address of packet.
- Interface—Unit/Slot/Interface on which packet is expected.
- Type—The possible field values are:
  - Dynamic—Entry has limited lease time.
  - Static—Entry was statically configured.
- Lease Time—If the entry is dynamic, enter the amount of time that the entry is to be active in the DHCP Database. If there's no Lease Time, check Infinite.)

Step 4 Click **Apply**. The settings are defined, and the device is updated.

Step 5 Click **Clear Dynamic** to delete the configuration.

DHCP Server

The DHCP Server feature enables you to configure the device as a DHCPv4 server. A DHCPv4 server is used to assign IPv4 address and other information to another device (DHCP client) The DHCPv4 server allocates IPv4 addresses from a user-defined pool of IPv4 addresses.

These can be in the following modes:

- Static Allocation—The hardware address or client identifier of a host is manually mapped to an IP address.
- Dynamic Allocation—A client obtains a leased IP address for a specified period of time (that can be infinite). If the DHCP client does not renew the allocated IP Address, the IP address is revoked at the end of this period, and the client must request another IP address.

DHCP Server Properties

To configure the device as a DHCPv4 server, follow these steps:

Procedure

Step 1 Click **IPv4 Configuration** > **DHCP Server** > **Properties** to display the Properties page.

Step 2 Select **Enable** to configure the device as a DHCP server.

Step 3 Click **Apply**. The device immediately begins functioning as a DHCP server. However, it does not assign IP addresses to clients until a pool is created.

Network Pools

When the device is serving as a DHCP server, one or more pools of IP addresses must be defined, from which the device allocates IP addresses to DHCP clients. Each network pool contains a range of addresses that belong to a specific subnet. These addresses are allocated to various clients within that subnet.

When a client requests an IP address, the device as DHCP server allocates an IP address according to the following:

- Directly Attached Client—The device allocates an address from the network pool whose subnet matches the subnet configured on the device's IP interface from which the DHCP request was received.

  If the message arrived directly (not via DHCP Relay) the pool is a Local pool and belongs to one of IP subnets defined on the input layer 2 interface. In this case, the IP mask of the pool equals to the IP mask of the IP interface and the minimum and maximum IP addresses of the pool belong to the IP subnet.

- Remote Client—The device takes an IP address from the network pool with the IP subnet that matches the IP address of the DHCP relay agent.

  If the message arrived via DHCP relay, the address used belongs to the IP subnet specified by minimum IP address and IP mask of the pool. That pool is a remote pool.

Up to 16 network pools can be defined.

To create a pool of IP addresses, and define their lease durations, follow these steps:

Procedure

Step 1 Click **IPv4 Configuration** > **DHCP Server** > **Network Pools**.

The previously defined network pools are displayed. These fields are described below in the Add page. The following field is displayed (but not in the Add page):

- Number of Leased Addresses—Number of addresses in the pool that have been assigned (leased).

Step 2 Click **Add** to define a new network pool. Note that you either enter the Subnet IP Address and the Mask, or enter the Mask, the Address Pool Start and Address Pool End.

Step 3 Enter the fields:

- Pool Name—Enter the pool name.
- Subnet IP Address—Enter the subnet in which the network pool resides.

- Mask—Enter one of following:
  - Network Mask—Check and enter the pool's network mask.
  - Prefix Length—Check and enter the number of bits that comprise the address prefix.
- Address Pool Start—Enter the first IP address in the range of the network pool.
- Address Pool End—Enter the last IP address in the range of the network pool.
- Lease Duration—Enter the amount of time a DHCP client can use an IP address from this pool. You can configure a lease duration of up to 49,710 days or an infinite duration.
  - Infinite—The duration of the lease is unlimited.
  - Days—The duration of the lease in number of days The ranges is 0–49,710 days.
  - Hours—The number of hours in the lease A days value must be supplied before an hours value can be added.
  - Minutes—The number of minutes in the lease A days value and an hours value must be added before a minutes value can be added.
- Default Router IP Address (Option 3)—Enter the default router for the DHCP client.
- Domain Name Server IP Address (Option 6)—Select one of the devices DNS servers (if already configured) or select **Other** and enter the IP address of the DNS server available to the DHCP client.
- Domain Name (Option 15)—Enter the domain name for a DHCP client.
- NetBIOS WINS Server IP Address (Option 44)—Enter the NetBIOS WINS name server available to a DHCP client.
- NetBIOS Node Type (Option 46)—Select how to resolve the NetBIOS name. Valid node types are:
  - Hybrid—A hybrid combination of b-node and p-node is used. When configured to use h-node, a computer always tries p-node first and uses b-node only if p-node fails. This is the default.
  - Mixed—A combination of b-node and p-node communications is used to register and resolve NetBIOS names. M-node first uses b-node; then, if necessary, p-node. M-node is typically not the best choice for larger networks because its preference for b-node. Broadcasts increase network traffic.
  - Peer-to-Peer—Point-to-point communications with a NetBIOS name server are used to register and resolve computer names to IP addresses.
  - Broadcast—IP Broadcast messages are used to register and resolve NetBIOS names to IP addresses.
- SNTP Server IP Address (Option 4)—Select one of the device's SNTP servers (if already configured) or select **Other** and enter the IP address of the time server for the DHCP client.
- File Server IP Address (siaddr)—Enter the IP address of the TFTP/SCP server from which the configuration file is downloaded.
- File Server Host Name (sname/Option 66)—Enter the name of the TFTP/SCP server.
- Configuration File Name (file/Option 67)—Enter the name of the file that is used as a configuration file.

Step 4 Click **Apply**. The Running Configuration file is updated.

Excluded Addresses

By default, the DHCP server assumes that all pool addresses in a pool may be assigned to clients. A single IP address or a range of IP addresses can be excluded. The excluded addresses are excluded from all DHCP pools.

To define an excluded address range, follow these steps:

Procedure

Step 1 Click **IPv4 Configuration** > **DHCP Server** > **Excluded Addresses**.

The previously defined excluded IP addresses are displayed.

Step 2 To add a range of IP addresses to be excluded, click **Add**, and enter the fields:

- Start IP Address—First IP address in the range of excluded IP addresses.
- End IP Address—Last IP address in the range of excluded IP addresses.

Step 3 Click **Apply**. The Running Configuration file is updated.

Static Hosts

You might want to assign some DHCP clients a permanent IP address that never changes. This client is then known as a static host. You can define up to 120 static hosts.

To manually allocate a permanent IP address to a specific client, complete the following steps:

Procedure

Step 1 Click **IPv4 Configuration** > **DHCP Server** > **Static Hosts**.

The static hosts are displayed. The fields displayed are described in the Add page, except for the following:

- MAC Address/Client Identifier

Step 2 To add a static host, click **Add**, and enter the fields:

IP Address	Enter the IP address that was statically assigned to the host.
Host Name	Enter the host name, which can be a string of symbols and an integer.
Mask	Enter the static host's network mask. • Network Mask—Check and enter the static host's network mask. • Prefix Length—Check and enter the number of bits that comprise the address prefix.

Identifier Type	Set how to identify the specific static host. • Client Identifier—Enter a unique identification of the client specified in hexadecimal notation, such as: 01b60819681172. Or: • MAC Address—Enter the MAC address of the client. Enter either the Client Identifier or MAC Address, according to which type you selected.
Client Name	Enter the name of the static host, using a standard set of ASCII characters. The client name must not include the domain name.
Default Router IP Address (Option 3)	Enter the default router for the static host.
Domain Name Server IP Address (Option 6)	Select one of the devices DNS servers (if already configured) or select **Other** and enter the IP address of the DNS server available to the DHCP client.
Domain Name (Option 15)	Enter the domain name for the static host.
NetBIOS WINS Server IP Address (Option 44)	Enter the NetBIOS WINS name server available to the static host.
NetBIOS Node Type (Option 46)	Select how to resolve the NetBIOS name. Valid node types are: • Hybrid—A hybrid combination of b-node and p-node is used. When configured to use h-node, a computer always tries p-node first and uses b-node only if p-node fails. This is the default. • Mixed—A combination of b-node and p-node communications is used to register and resolve NetBIOS names. M-node first uses b-node; then, if necessary, p-node. M-node is typically not the best choice for larger networks because its preference for b-node. Broadcasts increases network traffic. • Peer-to-Peer—Point-to-point communications with a NetBIOS name server are used to register and resolve computer names to IP addresses. • Broadcast—IP Broadcast messages are used to register and resolve NetBIOS names to IP addresses.
SNTP Server IP Address (Option 4)	Select one of the device's SNTP servers (if already configured) or select **Other** and enter the IP address of the time server for the DHCP client.
File Server IP Address (siaddr)	Enter the IP address of the TFTP/SCP server from which the configuration file is downloaded.
File Server Host Name (sname/Option 66)	Enter the name of the TFTP/SCP server.
Configuration File Name (file/Option 67)	Enter the name of the file that is used as a configuration file.

Step 3 Click **Apply**. The Running Configuration file is updated.

DHCP Options

When the device is acting as a DHCP server, the DHCP options can be configured using the HEX option. A description of these options can be found in RFC2131. The configuration of these options determines the reply that is sent to DHCP clients whose packets include a request (using option 55) for the configured DHCP options. Example: The DHCP option 66 is configured with the name of a TFTP server in the DHCP Options page. When a client DHCP packet is received containing option 66, the TFTP server is returned as the value of option 66.

To configure one or more DHCP options, follow these steps:

Procedure

Step 1 Click **IPv4 Configuration** > **DHCP Server** > **DHCP Options**.

The previously configured DHCP options are displayed.

Step 2 To configure an option that has not been configured yet, enter the field:

- DHCP Server Pool Name equals to—Select one of the pool of network addresses defined in the Network Pools, on page 221 and click **Go** to filter by that pool of network addresses.

Step 3 Click **Add** and enter the fields:

- Pool Name—Displays the name of the pool name for which code is being defined.
- Code—Enter the DHCP option code.
- Type—The radio buttons for this field, change according to the type of the DHCP option's parameter. Select one of the following codes and enter the value for the DHCP options parameter:
  - Hex—Select if you want to enter the hex value of the parameter for the DHCP option. A hex value can be provided in place of any other type of value. For instance, you can provide a hex value of an IP address instead of the IP address itself.

    No validation is made of the hex value, therefore if you enter a HEX value, which represents an illegal value, no error is provided, and the client might not be able to handle the DHCP packet from the server.
  - IP—Select if you want to enter an IP address when this is relevant for the DHCP option selected.
  - IP List—Enter list of IP addresses separated by commas.
  - Integer—Select if you want to enter an integer value of the parameter for the DHCP option selected.
  - Boolean—Select if the parameter for the DHCP option selected is Boolean.
- Boolean Value—If the type was Boolean, select the value to be returned: True or False.
- Value—If the type isn't Boolean, enter the value to be sent for this code.
- Description—Enter a text description for documentation purposes.

Step 4 Click **Apply**. The Running Configuration file is updated.

Address Binding

Use the Address Binding page to view and remove the IP addresses allocated by the device and their corresponding MAC addresses.

To view and/or remove address bindings, complete the following steps:

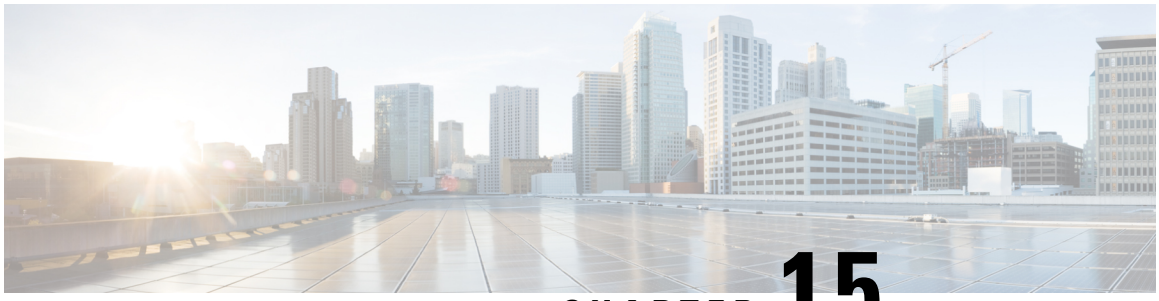
Procedure

Step 1 Click **IPv4 Configuration** > **DHCP Server** > **Address Binding**.

The following fields for the address bindings are displayed:

- IP Address—The IP addresses of the DHCP clients.
- Address Type—Whether the address of the DHCP client appears as a MAC address or using a client identifier.
- MAC Address/Client Identifier—A unique identification of the client specified as a MAC Address or in hexadecimal notation, e.g., 01b60819681172.
- Lease Expiration—The lease expiration date and time of the host's IP address or Infinite is such was the lease duration defined.
- Type—The manner in which the IP address was assigned to the client. The possible options are:
  - Static—The hardware address of the host was mapped to an IP address.
  - Dynamic—The IP address, obtained dynamically from the device, is owned by the client for a specified time. The IP address is revoked at the end of this period, when the client must request another IP address.
- State—The possible options are:
  - Allocated—IP address has been allocated. When a static-host is configured, its state is allocated.
  - Declined—IP address was offered but not accepted, therefore it's not allocated.
  - Expired—The lease of the IP address has expired.
  - Pre-allocated—An entry is in pre-allocated state from the time between the offer and the time that the DHCP ACK is sent from the client. Then it becomes allocated.

Step 2 Click **Delete**. The Running Configuration file is updated.



CHAPTER 15

IPv6 Configuration

This chapter contains the following sections:

- IPv6 Global Configuration, on page 227
- IPv6 Interfaces, on page 228
- IPv6 Tunnels, on page 230
- IPv6 Addresses, on page 232
- IPv6 Router Configuration, on page 233
- IPv6 Default Router List, on page 236
- IPv6 Neighbors, on page 237
- IPv6 Prefix List, on page 238
- IPv6 Access Lists, on page 240
- IPv6 Routes, on page 240
- DHCPv6 Relay, on page 241

IPv6 Global Configuration

The Internet Protocol version 6 (IPv6) is a network-layer protocol for packet-switched internetworks. IPv6 was designed to replace IPv4, the predominantly deployed Internet protocol. IPv6 introduces greater flexibility in assigning IP addresses, because the address size increases from 32-bit to 128-bit addresses. IPv6 addresses are written as eight groups of four hexadecimal digits, for example FE80:0000:0000:0000:0000:9C00:876A:130B. The abbreviated form, in which a group of zeroes can be left out, and replaced with '::', is also acceptable, for example, FE80::9C00:876A:130B. IPv6 interface addresses can be configured manually by the user, or automatically configured by a DHCP server.

This section provides information for defining the device IPv6 addresses, either manually or by making the device a DHCP client. To define IPv6 global parameters and DHCPv6 client settings, follow these steps:

Procedure

Step 1 Click **IPv6 Configuration** > **IPv6 Global Configuration**.

Step 2 Enter values for the following fields:

- IPv6 Routing—Select to enable IPv6 routing. If this isn't enabled, the device acts as a host (not a router) and can receive management packets, but can't forward packets. If routing is enabled, the device can forward the IPv6 packets.

  Enabling IPv6 routing removes any address previously assigned to the device interface, via the auto-config operation, from an RA sent by a Router in the network.

- ICMPv6 Rate Limit Interval—Enter how often the ICMP error messages are generated.
- ICMPv6 Rate Limit Bucket Size—Enter the maximum number of ICMP error messages that can be sent by the device per interval.
- IPv6 Hop Limit—Enter the maximum number of intermediate routers on its way to the final destination to which a packet can pass. Each time a packet is forwarded to another router, the hop limit is reduced. When the hop limit becomes zero, the packet is discarded. This prevents packets from being transferred endlessly.
- DHCPv6 Client Settings
  - Unique Identifier (DUID) Format—This is the identifier of the DHCP client that is used by the DHCP server to locate the client. It can be in one of the following formats:

    Link-Layer—(Default). If you select this option, the MAC address of the device is used.

    Enterprise Number—If you select this option, enter the following fields.

  - Enterprise Number—The vendors registered Private Enterprise number as maintained by IANA.
  - Identifier—The vendor-defined hex string (up to 64 hex characters) If the number of the character isn't even, a zero is added at the right. Each 2 hex characters can be separated by a period or colon.
- DHCPv6 Unique Identifier (DUID)—Displays the identifier selected.

Step 3 Click **Apply**. The IPv6 global parameters and DHCPv6 client settings are updated.

IPv6 Interfaces

The Internet Protocol version 6 (IPv6) is a network-layer protocol used for packet-switched internet communications.IPv6 was created to replace IPv4, the most widely used Internet protocol. Because the address size increases from 32-bit to 128-bit, IPv6 allows for greater flexibility in assigning IP addresses.IPv6 addresses are composed of eight groups of four hexadecimal digits, such as FE80:0000:0000:0000:0000:9C00:876A:130B.

To communicate with other IPv6 nodes over an IPv4-only network, IPv6 nodes require an intermediary mapping mechanism. This mechanism, known as a tunnel, allows IPv6-only hosts to access IPv4 services and isolated IPv6 hosts and networks to connect to an IPv6 node via the IPv4 infrastructure.

An IPv6 interface can be configured on a port, LAG, VLAN, loopback interface or tunnel. To define an IPv6 interface, follow these steps:

Procedure

Step 1 Click **IPv6 Configuration** > **IPv6 Interfaces**.

Step 2 Enter the parameters.

- IPv6 Link Local Default Zone—Select to enable defining a default zone. This is an interface to be used to egress a link-local packet arriving without a specified interface or with its default zone 0.
- IPv6 Link Local Default Zone Interface—Select an interface to be used as a default zone. This can be a previously defined tunnel or other interface.

Step 3 Click **Apply** to configure default zone.

The IPv6 Interface Table is displayed along with the following field:

- Tunnel Type—Manual, 6–4 and ISATAP.

Step 4 Click **Add** to add a new interface on which interface IPv6 is enabled.

Step 5 Enter the fields:

- IPv6 Interface—Select a specific port, LAG, loopback interface or VLAN for the IPv6 address.

Step 6 To configure the interface as a DHCPv6 client, meaning to enable the interface to receive information from the DHCPv6 server, such as: SNTP configuration and DNS information, enter the DHCPv6 Client fields:

- DHCPv6 Client—Select to enable DHCPv6 Client (stateless and stateful) on the interface.
- Rapid Commit—Select to enable the use of the two-message exchange for address allocation and other configuration. If it's enabled, the client includes the rapid-commit option in a solicit message.
- Minimum Information Refresh Time—This value is used to put a floor on the refresh time value. If the server sends a refresh time option that is less than this value, this value is used instead. Select Infinite or User Defined to set a value.
- Information Refresh Time—This value indicates how often the device refreshes information received from the DHCPv6 server. If this option isn't received from the server, the value entered here is used. Select Infinite or User Defined to set a value.

Step 7 To configure additional IPv6 parameters, enter the following fields:

- IPv6 Address Auto Configuration—Select to enable automatic address configuration from router advertisements sent by neighbors.
- Number of DAD Attempts—Enter the number of consecutive neighbor solicitation messages that are sent while Duplicate Address Detection (DAD) is performed on the interface's Unicast IPv6 addresses. DAD verifies the uniqueness of a new Unicast IPv6 address before it's assigned. New addresses remain in a tentative state during DAD verification. Entering 0 in this field disables duplicate address detection processing on the specified interface. Entering 1 in this field indicates a single transmission without follow-up transmissions.
- Send ICMPv6 Messages—Enable generating unreachable destination messages.
- IPv6 Redirects—Select to enable sending ICMP IPv6 redirect messages. These messages inform other devices not to send traffic to the device, but rather to another device.

Step 8 Click **Apply** to enable IPv6 processing on the selected interface. Regular IPv6 interfaces have the following addresses automatically configured:

- Link local address using EUI-64 format interface ID based on a device's MAC address

- All node link local Multicast addresses (FF02::1)
- Solicited-Node Multicast address (format FF02::1:FFXX:X)

Step 9 Select an Interface and click **Restart** to initiate a refresh of the stateless information received from the DHCPv6 server.

Step 10 Select an interface and click **Details** to display the information received on the interface from a DHCPv6 server.

Step 11 Click **IPv6 Address Table** to manually assign IPv6 addresses to the interface, if required.

Step 12 To add a tunnel, select an interface in the IPv6 Tunnel Table and click **IPv6 Tunnel**.

IPv6 Tunnels

Tunnels enable transmission of IPv6 packets over IPv4 networks. Each tunnel has a source IPv4 address and if it's a manual tunnel it also has a destination IPv4 address. The IPv6 packet is encapsulated between these addresses.

ISATAP Tunnels

The device supports a single Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnel. An ISATAP tunnel is a point-to-multi-point tunnel. The source address is the IPv4 address (or one of the IPv4 addresses) of the device. When configuring an ISATAP tunnel, the destination IPv4 address is provided by the router. Note that:

- An IPv6 link local address is assigned to the ISATAP interface. The initial IP address is assigned to the interface, which is then activated.
- If an ISATAP interface is active, the ISATAP router IPv4 address is resolved via DNS by using ISATAP-to-IPv4 mapping. If the ISATAP DNS record is not resolved, ISATAP host name-to-address mapping is searched in the host mapping table
- When the ISATAP router IPv4 address is not resolved via the DNS process, the ISATAP IP interface remains active. The system does not have a default router for ISATAP traffic until the DNS process is resolved.

Additional Types of Tunnels

The following additional types of tunnels can be configured on the device:

Manual Tunnel

- An IPv6 link local address is assigned to the ISATAP interface. The initial IP address is assigned to the interface, which is then activated
- If an ISATAP interface is active, the ISATAP router IPv4 address is resolved via DNS by using ISATAP-to-IPv4 mapping. If the ISATAP DNS record is not resolved, ISATAP host name-to-address mapping is searched in the host mapping table.
- When the ISATAP router IPv4 address is not resolved via the DNS process, the ISATAP IP interface remains active. The system does not have a default router for ISATAP traffic until the DNS process is resolved.

This is a point-to-point definition. When creating a manual tunnel, you enter both the source IP address (one of the device's IP addresses) and the destination IPv4 address.

6 to 4 Tunnel

- 6 to 4 is an automatic tunneling mechanism that uses the underlying IPv4 network as a non-Broadcast multiple-access link layer for IPv6. Only one 6 to 4 tunnel is supported on a device.
- The 6 to 4 tunnel is supported only when IPv6 Forwarding is supported.
- IPv6 Multicast is not supported on the 6to4 tunnel interface
- The switch automatically creates a 2002::/16 on-link prefix on the 6to4 tunnel. The connected 2002::/16 route on the tunnel is added to the Routing Table as result of the on-link prefix creation
- When the tunnel mode is changed from 6to4 to another mode, the on-link prefix and connected routes are removed.
- When the next hop outgoing interface is the 6to4 tunnel, the IPv4 address of the next hop node is taken from the prefix 2002:WWXX:YYZZ::/48 of the IPv6 next hop IPv6 address, if it is global, and from the last 32 bits of the interface identifier of the IPv6next hop IPv6 address, if it is link local.

The following table summarizes tunnel support in the various devices:

Tunnel Type	CBS350	CBS350 Stacking
ISATAP	Supported	Supported
Manual	Not Supported	Not Supported
Automatic 6to4 tunnel	Not Supported	Not Supported

To configure an IPv6 tunnel follow these steps:

Procedure

Step 1 Click **IPv6 Configuration >IPv6 Tunnel**.

Step 2 Click **Create ISATAP Tunnel.**

Step 3 The Tunnel Number (1) and its Tunnel Type (ISATAP) are displayed.

Step 4 Enter the following fields

- Source IPv4 Address—Set the local (source) IPv4 address of a tunnel interface. The IPv4 address of the selected IPv4 interface is used to form part of the IPv6 address over the ISATAP tunnel interface. The IPv6 address has a 64-bit network prefix of fe80::, with the rest of the 64-bit formed by concatenating 0000:5EFE and the IPv4 address.
  - Auto—Automatically selects the lowest IPv4 address from among all of its configured IPv4 interfaces as the source address for packets sent on the tunnel interface.
  - Manual—Specifies the IPv4 address to use as the source address for packets sent on the tunnel interface. The local address of the tunnel interface is not changed when the IPv4 address is moved to another interface.

    Note
    If the device IPv4 address is changed, the local address of the tunnel interface is also changed

- Interface—Specifies the interface

- ISATAP Router Name— Select one of the following options to configure a global string that represents a specific automatic tunnel router domain name.
  - Use Default—This is always ISATAP.
  - User Defined—Enter the router's domain name.

Step 5 Enter the parameters:

- ISATAP Solicitation Interval—The number of seconds between ISATAP router solicitations messages, when no active ISATAP router is discovered. The interval can be the Default Value or a User Defined interval.
- ISATAP Robustness—Used to calculate the interval for router solicitation queries. The bigger the number, the more frequent the queries. The interval can be the Default Value or a User Defined interval .

Note
The ISATAP tunnel is not operational if the underlying IPv4 interface is not in operation.

Step 6 Click **Apply** to save the ISATAP parameters to the Running Configuration file.

IPv6 Addresses

To assign an IPv6 address to an IPv6 Interface, follow these steps:

Procedure

Step 1 Click **IPv6 Configuration** > **IPv6 Addresses**.

Step 2 To filter the table, select an interface name, and click **Go**. The interface appears in the IPv6 Address Table. These fields are described in the Add page except for the following fields:

- Address Source—Displays one of the address source types: DHCP, System or Static.
- IPv6 Address Type—Displays the type of IPv6 address.
- IPv6 Address—Displays the IPv6 address.
- Preferred Lifetime—Displays the entry preferred lifetime.
- Valid Lifetime—Displays the entry valid lifetime.
- Expiry Time—Displays the expiry time.

Step 3 Click **Add**.

Step 4 Enter values for the fields.

Option	Description
IPv6 Interface	Displays the interface on which the IPv6 address is to be defined. If an * is displayed, this means that the IPv6 interface is not enabled but has been configured.
IPv6 Address Type	Select the type of the IPv6 address to add. • Link Local—An IPv6 address that uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration. • Global—An IPv6 address that is a global Unicast IPV6 type that is visible and reachable from other networks. • Anycast—The IPv6 address is an Anycast address. This is an address that is assigned to a set of interfaces that typically belong to different nodes. A packet sent to an Anycast address is delivered to the closest interface—as defined by the routing protocols in use—identified by the Anycast address. **Note** Anycast cannot be used, if the IPv6 address is on an ISATAP interface.
IPv6 Address	In addition to the default link local and Multicast addresses, the device also automatically adds global addresses to the interface based on the router advertisements it receives. The device supports a maximum of 128 addresses at the interface. Each address must be a valid IPv6 address that is specified in hexadecimal format by using 16-bit values separated by colons.
Prefix Length	The length of the Global IPv6 prefix is a value from 0-128 indicating the number of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
EUI-64	Select to use the EUI-64 parameter to identify the interface ID portion of the Global IPv6 address by using the EUI-64 format based on a device MAC address.

Step 5 Click **Apply**. The Running Configuration file is updated.

IPv6 Router Configuration

The following sections describe how to configure IPv6 routers. It covers the following topics:

Router Advertisement

A router advertisement packet contains various configurations for IPv6 hosts including the network part of the layer 3 IPv6 address required by hosts to communicate in the internet. Clients then generate the universally unique host part of the address and derive the complete address. This feature can be enabled or suppressed per interface, as follows:

Procedure

Step 1 Click **IPv6 Configuration** > **IPv6 Router Configuration** > **Router Advertisement**.

Step 2 To configure an interface listed in the Router Advertisement Table, select it and click **Edit**.

Step 3 Enter the following fields:

Option	Description
Suppress Router Advertisement	Select Yes to suppress IPv6 router advertisement transmissions on the interface.
Router Preference	Select either Low, Medium or High preference for the router. Router advertisement messages are sent with the preference configured in this field. If no preference is configured, they are sent with a medium preference.
Include Advertisement Interval Option	Select to indicate that an advertisement option will be used by the system. This option indicates to a visiting mobile node the interval at which that node may expect to receive router advertisements. The node may use this information in its movement detection algorithm.
Hop Limit	This is the value that the router advertises. If it's not zero, it's used as the hop limit by the host.
Managed Address Configuration Flag	Select this flag to indicate to attached hosts that they should use stateful auto configuration to obtain addresses. Hosts may use stateful and stateless address auto configuration simultaneously.
Other Stateful Configuration Flag	Other Stateful Configuration Flag—Select this flag to indicate to attached hosts that they should use stateful auto configuration to obtain other (non-address) information. **Note** If the Managed Address Configuration flag is set, an attached host can use stateful auto configuration to obtain the other (non-address) information regardless of the setting of this flag.
Neighbor Solicitation Retransmissions Interval	Enter the interval to determine the time between retransmissions of neighbor solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor (User Defined), or select Use Default to use the system default (1000).
Maximum Router Advertisement Interval	Enter the maximum amount of time that can pass between router advertisements. The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if you configure the route as a default router by using this command. To prevent synchronization with other IPv6 nodes, the actual interval used is randomly selected from a value between the minimum and maximum values.
Minimum Router Advertisement Interval	Enter the minimum amount of time that can pass between router advertisements (User Defined) or select Use Default to user the system default. **Note** The minimum RA interval may never be more than 75% of the maximum RA interval and never less than 3 seconds.

Option	Description
Router Advertisement Lifetime	Enter the remaining length of time, in seconds, that this router remains useful as a default router. A value of zero indicates that it's no longer useful as a default router.
Reachable Time	Enter the amount of time that a remote IPv6 node is considered reachable (in milliseconds) (User Defined) or select the Use Default option to use the system default.

Step 4 Click **Apply** to save the configuration to the Running Configuration file.

IPv6 Prefixes

To define prefixes to be advertised on the interfaces of the device, follow these steps:

Procedure

Step 1 Click **IPv6 Configuration** > **IPv6 Router Configuration** > **IPv6 Prefixes**.

Step 2 If required, enable the Filter field and click **Go**. The group of interfaces matching the filter are displayed.

Step 3 To add an interface, click **Add.**

Step 4 Select the required IPv6 Interface on which a prefix is to be added.

Step 5 Enter the following fields:

Option	Description
Prefix Address	The IPv6 network. This argument must be in the form documented in RFC 4293 where the address is specified in hexadecimal—using 16-bit values between colons.
Prefix Length	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
Prefix Advertisement	Select to advertise this prefix.
Valid Lifetime	The remaining length of time, in seconds, that this prefix will continue to be valid, i.e., time until invalidation. The address generated from an invalidated prefix should not appear as the destination or source address of a packet. • Infinite—Select this value to set the field to 4,294,967,295, which represents infinity. • User Defined—Enter a value.
Preferred Lifetime	The remaining length of time, in seconds, that this prefix will continue to be preferred. After this time has passed, the prefix should no longer be used as a source address in new communications, but packets received on such an interface are processed as expected. The preferred-lifetime must not be larger than the valid-lifetime. • Infinite—Select this value to set the field to 4,294,967,295, which represents infinity. • User Defined—Enter a value.

Option	Description
Auto Configuration	Enable automatic configuration of IPv6 addresses using stateless auto configuration on an interface and enable IPv6 processing on the interface. Addresses are configured depending on the prefixes received in Router Advertisement messages.
Prefix Status	Select one of the following options: • Onlink—Configures the specified prefix as on-link. Nodes sending traffic to addresses that contain the specified prefix consider the destination to be locally reachable on the link. An onlink prefix is inserted into the routing table as a connected prefix (L-bit set). • No-Onlink—Configures the specified prefix as not onlink. A no onlink prefix is inserted into the routing table as a connected prefix but advertised with a L-bit clear. • Offlink—Configures the specified prefix as offlink. The prefix will be advertised with the L-bit clear. The prefix will not be inserted into the routing table as a connected prefix. If the prefix is already present in the routing table as a connected prefix (for example, because the prefix was also configured by adding an IPv6 address), it will be removed.

Step 6 Click **Apply** to save the configuration to the Running Configuration file.

IPv6 Default Router List

The IPv6 Default Router List page enables configuring and viewing the default IPv6 router addresses. This list contains the routers that are candidates to become the device default router for non-local traffic (it may be empty). The device randomly selects a router from the list. The device supports one static IPv6 default router. Dynamic default routers are routers that have sent router advertisements to the device IPv6 interface.

When adding or deleting IP addresses, the following events occur:

- When removing an IP interface, all the default router IP addresses are removed. Dynamic IP addresses can’t be removed.
- An alert message appears after an attempt is made to insert more than a single user-defined address.
- An alert message appears when attempting to insert a non-link local type address, meaning 'fe80:'.

To define a default router, complete the following:

Procedure

Step 1 Click **IPv6 Configuration** > **IPv6 Default Router List**.

This page displays the following fields for each default router:

- Outgoing Interface—Outgoing IPv6 interface where the default router resides.
- Default Router IPv6 Address—Link local IP address of the default router.
- Type—The default router configuration that includes the following options:

- Static—The default router was manually added to this table through the Add button.
- Dynamic—The default router was dynamically configured.
- Neighbor Discovery (ND)—The default router is set to ND. Neighbor Discovery Protocol is used to identify the relationships between the different neighboring devices in an IPv6 network.

- Metric—Cost of this hop.

Step 2 Click **Add** to add a static default router.

Step 3 Enter the following fields:

- Next Hop Type—The IP address of the next destination to which the packet is sent. This is composed of the following:
  - Global—An IPv6 address that is a global Unicast IPV6 type that is visible and reachable from other networks.
  - Link Local—An IPv6 interface and IPv6 address that uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
- Outgoing Interface—Displays the outgoing Link Local interface.
- Default Router IPv6 Address—The IP address of the static default router
- Metric—Enter the cost of this hop.

Step 4 Click **Apply**. The default router is saved to the Running Configuration file.

IPv6 Neighbors

The IPv6 Neighbors page enables configuring and viewing the list of IPv6 neighbors on the IPv6 interface. The IPv6 Neighbor Table (also known as IPv6 Neighbor Discovery Cache) displays the MAC addresses of the IPv6 neighbors that are in the same IPv6 subnet as the device. This is the IPv6 equivalent of the IPv4 ARP Table. When the device needs to communicate with its neighbors, the device uses the IPv6 Neighbor Table to determine the MAC addresses based on their IPv6 addresses.

This page displays the neighbors that automatically detected or manually configured entries. Each entry displays to which interface the neighbor is connected, the neighbor's IPv6 and MAC addresses, the entry type (static or dynamic), and the state of the neighbor.

To define IPv6 neighbors, complete the following steps:

Procedure

Step 1 Click **IPv6 Configuration** > **IPv6 Neighbors**.

You can select an option to clear some or all of the IPv6 addresses in the Clear Table section.

- Static Only—Deletes the static IPv6 address entries.

- Dynamic Only—Deletes the dynamic IPv6 address entries.
- All Dynamic & Static—Deletes the static and dynamic address entries IPv6 address entries.

Step 2 To add a neighbor to the table, click **Add**.

Step 3 The following fields are displayed:

- Interface—Displays the neighboring IPv6 interface to be added.
- IPv6 Address—Enter the IPv6 network address assigned to the interface. The address must be a valid IPv6 address.
- MAC Address—Enter the MAC address mapped to the specified IPv6 address.

Step 4 Click **Apply**. The Running Configuration file is updated.

Step 5 Next, you will see the following settings displayed in the IPv6 Neighbor Table.

- Interface—Neighboring IPv6 interface type.
- IPv6 Address—IPv6 address of a neighbor.
- MAC Address—MAC address mapped to the specified IPv6 address.
- Type—Neighbor discovery cache information entry type (static or dynamic).
- State—Specifies the IPv6 neighbor status. The values are:
  - Incomplete—Address resolution is working. The neighbor has not yet responded.
  - Reachable—Neighbor is known to be reachable.
  - Stale—Previously-known neighbor is unreachable. No action is taken to verify its reachability until traffic must be sent.
  - Delay—Previously-known neighbor is unreachable. The interface is in Delay state for a predefined Delay Time. If no reachability confirmation is received, the state changes to Probe.
  - Probe—Neighbor is no longer known to be reachable, and Unicast Neighbor Solicitation probes are being sent to verify the reachability.
- Router—Specifies whether the neighbor is a router (Yes or No).

Step 6 To change the type of an IP address from Static to Dynamic, select the address, click **Edit** and use the Edit IPv6 Neighbors page.

IPv6 Prefix List

Prefix lists are configured with permit or deny keywords to either permit or deny a prefix based on a matching condition. An implicit deny is applied to traffic that doesn't match any prefix-list entry. A prefix-list entry consists of an IP address and a bit mask. The IP address can be for a classful network, a subnet, or a single host route. The bit mask is a number 1–32.

Prefix lists are configured to filter traffic based on a match of an exact prefix length or a match within a range when the ge and le keywords are used.

To create a prefix list, follow these steps:

Procedure

Step 1 Click **IPv6 Configuration** > **IPv6 Prefix List**.

Step 2 Click **Add**.

Step 3 Enter the following fields:

- List Name—Select one of the following options:
  - Use existing list—Select a previously defined list to add a prefix to it.
  - Create new list—Enter a name to create a new list.
- Sequence Number—Specifies the place of the prefix within the prefix list. Select one of the following options:
  - Auto Numbering—Puts the new IPV6 prefix after the last entry of the prefix list. The sequence number equals the last sequence number plus 5. If the list is empty the first prefix-list entry is assigned the number 5 and subsequent prefix list entries increment by 5.
  - User Defined—Puts the new IPV6 prefix into the place specified by the parameter. If an entry with the number exists, it's replaced by the new one.
- Rule Type—Enter the rule for the prefix list:
  - Permit—Permits networks that match the condition.
  - Deny—Denies networks that match the condition.
  - Description—Text
- IPv6 Prefix—IP route prefix.
- Prefix Length—IP route prefix length.
- Greater Than—Minimum prefix length to be used for matching. Select one of the following options:
  - No Limit—No minimum prefix length to be used for matching.
  - User Defined—Minimum prefix length to be matched.
- Lower Than—Maximum prefix length to be used for matching. Select one of the following options:
  - No Limit—No maximum prefix length to be used for matching.
  - User Defined—Maximum prefix length to be matched.
- Description—Enter a description of the prefix list.

Step 4 Click **Apply** to save the configuration to the Running Configuration file.

IPv6 Access Lists

The IPv6 access list can be used in MLD Proxy > Global MLD Proxy Settings > SSM IPv6 Access List page.

To create an access list, complete the following steps:

Procedure

Step 1 Click **IPv6 Configuration > IPv6 Access List**. To see a subset of entries in the list, enter the relevant search criteria in the filter and click **Go**.

Step 2 To add a new Access List, click **Add** and enter the following fields:

- Access List Name—Select one of the following:
  - Use existing list—Select a previously-existing access list.
  - Create new list—Enter a name for the new access list.
- Source IPv6 Address—Enter the source IPv6 address. The following options are available:
  - Any—All IP addresses are included.
  - User Defined—Enter an IP address.
- Prefix length—Enter the source IPv6 prefix length:
- Action—Select an action for the access list. The following options are available:
  - Permit—Permit entry of packets from the IP address(es) in the access list.
  - Deny—Reject entry of packets from the IP address(es) in the access list.

Step 3 Click **Apply**. The settings are written to the Running Configuration file.

IPv6 Routes

The IPv6 Forwarding Table contains the various routes that have been configured. One of these routes is a default route (IPv6 address: 0) that uses the default router selected from the IPv6 Default Router List to send packets to destination devices that aren't in the same IPv6 subnet as the device. In addition to the default route, the table also contains dynamic routes that are ICMP redirect routes received from IPv6 routers by using ICMP redirect messages. This could happen when the default router the device uses isn't the router for traffic to which the IPv6 subnets that the device wants to communicate.

To view IPv6 routes:

Click **IPv6 Configuration** > **IPv6 Routes**.

This page displays the following fields:

- IPv6 Prefix—IP route address prefix for the destination IPv6 subnet address

- Prefix Length—IP route prefix length for the destination IPv6 subnet address It's preceded by a forward slash.
- Outgoing Interface—Interface used to forward the packet.
- Next Hop—Type of address to which the packet is forwarded. Typically, this is the address of a neighboring router. It can be one of the following types.
  - Link Local—An IPv6 interface and IPv6 address that uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—An IPv6 address that is a global Unicast IPV6 type that is visible and reachable from other networks.
  - Point-to-Point—A Point-to-point tunnel
- Metric—Value used for comparing this route to other routes with the same destination in the IPv6 router table All default routes have the same value.
- Lifetime—Time period during which the packet can be sent, and resent, before being deleted.
- Route Type—How the destination is attached, and the method used to obtain the entry. The following values are:
  - S (Static)—Entry was manually configured by a user.
  - I (ICMP Redirect)—Entry is an ICMP redirect dynamic route received from an IPv6 router by using ICMP redirect messages.
  - ND (Router Advertisement)—Entry is taken from a router advertisement message.

Procedure

Step 1 To add a new route, click **Add** and enter the fields described above. In addition, enter the following field:

- IPv6 Address—Add the IPv6 address of the new route.

Step 2 Click **Apply** to save the changes.

DHCPv6 Relay

DHCPv6 Relay is used for relaying DHCPv6 messages to DHCPv6 servers. It's defined in RFC 3315.

When the DHCPv6 client isn't directly connected to the DHCPv6 server, a DHCPv6 relay agent (the device) to which this DHCPv6 client is directly-connected encapsulates the received messages from the directly connected DHCPv6 client, and forwards them to the DHCPv6 server.

In the opposite direction, the relay agent decapsulates packets received from the DHCPv6 server and forwards them, towards the DHCPv6 client.

The user must configure the list DHCP servers to which packets are forwarded. Two sets of DHCPv6 servers can be configured:

- Global Destinations—Packets are always relayed to these DHCPv6 servers.
- Interface List—This is a per-interface list of DHCPv6 servers. When a DHCPv6 packet is received on an interface, the packet is relayed both to the servers on the interface list (if it exists) and to the servers on the global destination list.

Global Destinations

To configure a list of DHCPv6 servers to which all DHCPv6 packets are relayed, complete the following steps:

Procedure

Step 1 Click **IPv6 Configuration** > **DHCPv6 Relay** > **Global Destinations**.

Step 2 To add a default DHCPv6 server, click **Add**.

Step 3 Enter the fields:

- IPv6 Address Type—Enter the type of the destination address to which client messages are forwarded. The address type can be Link Local, Global, or Multicast (All_DHCP_Relay_Agents_and_Servers).
- DHCPv6 Server IP Address—Enter the address of the DHCPv6 server to which packets are forwarded.
- IPv6 Interface—Enter the destination interface on which packets are transmitted when the address type of the DHCPv6 server is Link Local or Multicast. The interface can be a VLAN, LAG, or tunnel.

Step 4 Click **Apply**. The Running Configuration file is updated.

Interface Settings

To enable the DHCPv6 Relay feature on an interface and to configure a list of DHCPv6 servers, follow these steps:

Procedure

Step 1 Click **IPv6 Configuration** > **DHCPv6 Relay** > **Interface Settings**.

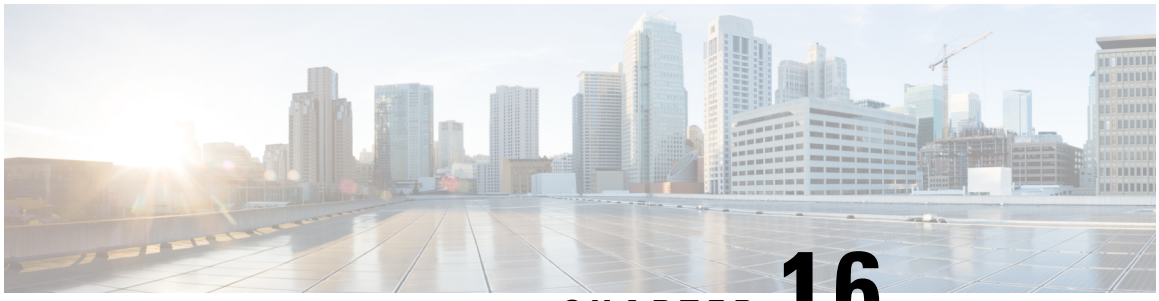
Step 2 To enable DHCPv6 on an interface and optionally add a DHCPv6 server for an interface, click **Add**.

Enter the fields:

- Source Interface—Select the interface (port, LAG, VLAN, or tunnel) for which DHCPv6 Relay is enabled.
- Use Global Destinations Only—Select to forward packets to the DHCPv6 global destination servers only.

- IPv6 Address Type—Enter the type of the destination address to which client messages are forwarded. The address type can be Link Local, Global, or Multicast (All_DHCP_Relay_Agents_and_Servers).
- DHCPv6 Server IP Address—Enter the address of the DHCPv6 server to which packets are forwarded.
- Destination IPv6 Interface— Select the destination IPv6 Interface from the drop-down menu.

Step 3 Click **Apply**. The Running Configuration file is updated.



CHAPTER 16

General IP Configuration

IP interface addresses can be configured manually by the user, or automatically configured by a DHCP server. This section provides information for defining the device IP addresses, either manually or by making the device a DHCP client.

- Policy-Based Routing, on page 245
- Domain Name System, on page 247

Policy-Based Routing

Policy-based Routing (PBR) provides a means for routing selected packets to a next hop address based on packet fields, using ACLs for classification. PBR lessens reliance on routes derived from routing protocols.

Route Maps

Route maps are the means used to configure PBR.

To add a route map, complete the following steps:

Procedure

Step 1 Click **General IP Configuration** > **Policy Based Routing** > **Route Maps**.

Step 2 Click **Add** and enter the parameters:

- Route Map Name—Select one of the following options for defining a route map:
  - Use existing map—Select a route map that was previously defined to add a new rule to it.
  - Create new map—Enter the name of a new route map.
- Sequence Number—Number that indicates the position/priority of rules in a specified route map. If a route map has more than one rule (ACL) defined on it, the sequence number determines the order in which the packets will be matched against the ACLs (from lower to higher number).
- Route Map IP Type—Select either IPv6 or IPv4 depending on the type of the next hop IP address.
- Match ACL—Select a previously defined ACL. Packets will be matched to this ACL.

- IPv6 Next Hop Type—If the next hop address is an IPv6 address, select one of the following characteristics:
  - Global—An IPv6 address that is a global Unicast IPV6 type that is visible and reachable from other networks.
  - Link Local—An IPv6 interface and IPv6 address that uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network.
- Interface—Displays the outgoing Link Local interface.
- Next Hop—IP address of the next hop router.

Step 3 Click **Apply**. The Running Configuration file is updated.

Route Map Binding

All packets coming in on an interface that is bound to a route map and match a route map rule are routed to the next hop defined in the rule.

To bind an interface to a route map, complete the following steps:

Procedure

Step 1 Click **General IP Configuration** > **Policy Based Routing** > **Route Map Binding**.

Step 2 Click **Add** and enter the parameters:

- Interface—Select an interface (with an IP address).
- Bound IPv4 Route Map—Select an IPv4 route map to bind to the interface.
- Bound IPv6 Route Map—Select an IPv6 route map to bind to the interface.

Step 3 Click **Apply**. The Running Configuration file is updated.

Policy-Based Routes

To view the route maps that defined, complete the following steps:

Procedure

Step 1 Click **General IP Configuration** > **Policy Based Routing** > **Policy Based Routes**.

Step 2 Previously-defined route maps are displayed:

- Interface Name—Interface on which route map is bound.
- Route Map Name—Name of route map.

- Route Map Status—Status of interface:
  - Active—Interface is up.
  - Interface Down—Interface is down.
- ACL Name—ACL associated with route map.
- Next Hop—Where packets matching route map will be routed.
- Next Hop Status—Reachability of next hop:
  - Active—The next hop IP address is reachable.
  - Unreachable—The status isn't active the next hop IP address isn't reachable.
  - Not Direct—The status isn't active because the next hop IP address isn't directly attached to a device subnet.

Domain Name System

The Domain Name System (DNS) translates domain names into IP addresses for the purpose of locating and addressing hosts.

As a DNS client, the device resolves domain names to IP addresses through the use of one or more configured DNS servers.

DNS Settings

Use the DNS Settings page to enable the DNS feature, configure the DNS servers and set the default domain used by the device. To configure the DNS Settings, follow these steps;

Procedure

Step 1 Click **General IP Configuration** > **DNS** > **DNS Settings**.

Step 2 In Basic Mode, enter the parameters:

- Server Definition—Select one of the following options for defining the DNS server:
  - By IP Address—IP Address will be entered for DNS server.
  - Disabled—No DNS server will be defined.
- Server IP Address—If you selected By IP Address above, enter the IP address of the DNS server.
- Default Domain Name—Enter the DNS domain name used to complete unqualified host names. The device appends this to all nonfully qualified domain names (NFQDNs) turning them into FQDNs.

  Note
  Don't include the initial period that separates an unqualified name from the domain name (like cisco.com).

Step 3 In Advanced Mode, enter the parameters.

- DNS—Select to designate the device as a DNS client, which can resolve DNS names into IP addresses through one or more configured DNS servers.
- Polling Retries—Enter the number of times to send a DNS query to a DNS server until the device decides that the DNS server doesn't exist.
- Polling Timeout—Enter the number of seconds that the device waits for a response to a DNS query.
- Polling Interval—Enter how often (in seconds) the device sends DNS query packets after the number of retries has been exhausted.
  - Use Default—Select to use the default value.

    This value = 2*(Polling Retries + 1)* Polling Timeout
  - User Defined—Select to enter a user-defined value.
- Default Parameters—Enter the following default parameters:
  - Default Domain Name—Enter the DNS domain name used to complete unqualified host names. The device appends this to all nonfully qualified domain names (NFQDNs) turning them into FQDNs.

    Note
    Don't include the initial period that separates an unqualified name from the domain name (like cisco.com).
  - DHCP Domain Search List—Click **Details** to view the list of DNS servers configured on the device.

Step 4 Click **Apply**. The Running Configuration file is updated.

The DNS Server Table displays the following information for each DNS server configured:

- DNS Server—The IP address of the DNS server.
- Preference—Each server has a preference value, a lower value means a higher chance of being used.
- Source—Source of the server's IP address (static or DHCPv4 or DHCPv6)
- Interface—Interface of the server's IP address.

Step 5 Up to eight DNS servers can be defined. To add a DNS server, click **Add.**

Step 6 Enter the parameters.

- IP Version—Select Version 6 for IPv6 or Version 4 for IPv4.
- IPv6 Address Type—Select the IPv6 address type (if IPv6 is used). The options are:
  - Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- Link Local Interface—If the IPv6 address type is Link Local, select the interface through which it's received.
- DNS Server IP Address—Enter the DNS server IP address.

- Preference—Select a value that determines the order in which the domains are used (from low to high). This effectively determines the order in which unqualified names are completed during DNS queries.

Step 7 Click **Apply**. The DNS server is saved to the Running Configuration file.

Search List

The search list can contain one static entry defined by the user in the DNS Settings, on page 247 and dynamic entries received from DHCPv4 and DHCPv6 servers.

To view the domain names that have been configured on the device, click **General IP Configuration** > **DNS** > **Search List**.

The following fields are displayed for each DNS server configured on the device.

- Domain Name—Name of domain that can be used on the device.
- Source—Source of the server's IP address (static or DHCPv4 or DHCPv6) for this domain.
- Interface—Interface of the server's IP address for this domain.
- Preference—This is the order in which the domains are used (from low to high). This effectively determines the order in which unqualified names are completed during DNS queries.

Host Mapping

Host name/IP address mappings are stored in the Host Mapping Table (DNS cache).

This cache can contain the following type of entries:

- Static Entries—These are mapping pairs that manually added to the cache. There can be up to 64 static entries.
- Dynamic Entries—Are mapping pairs that are either added by the system as a result of being used by the user, or an entry for each IP address configured on the device by DHCP. There can be 256 dynamic entries.

Name resolution always begins by checking static entries, continues by checking the dynamic entries, and ends by sending requests to the external DNS server. Eight IP addresses are supported per DNS server per host name.

To add a host name and its IP address, complete the following:

Procedure

Step 1 Click **General IP Configuration** > **DNS** > **Host Mapping**.

Step 2 If required, select one of the following options from Clear Table to clear some or all of the entries in the Host Mapping Table.

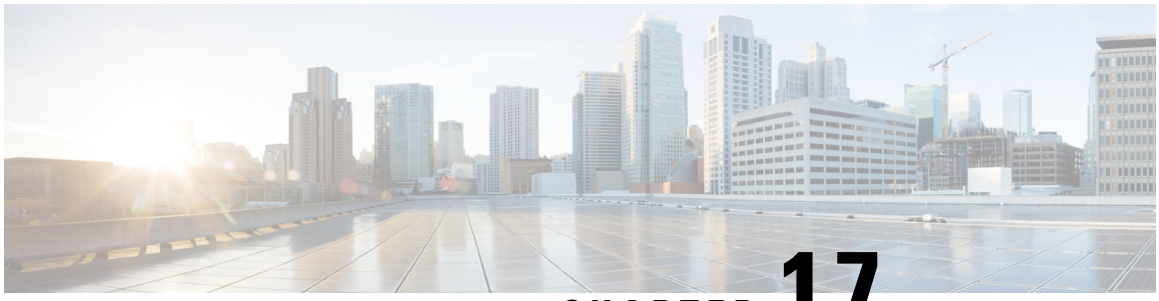
- Static Only—Deletes the static hosts.

- Dynamic Only—Deletes the dynamic hosts.
- All Dynamic & Static—Deletes the static and dynamic hosts.

Step 3 To add a host mapping, click **Add** and configure the following:

- IP Version—Select Version 6 for IPv6 or Version 4 for IPv4.
- IPv6 Address Type—Select the IPv6 address type (if IPv6 is used). The options are:
  - Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- Link Local Interface—If the IPv6 address type is Link Local, select the interface through which it's received.
- Host Name—Enter a user-defined host name or fully qualified name. Host names are restricted to the ASCII letters A through Z (case-insensitive), the digits 0–9, the underscore, and the hyphen. A period (.) is used to separate labels.
- IP Address—Enter a single address or up to eight associated IP addresses (IPv4 or IPv6).

Step 4 Click **Apply**. The settings are saved to the Running Configuration file.



CHAPTER 17

Security

This chapter contains the following sections:

- TACACS+ Client, on page 251
- RADIUS Client, on page 253
- RADIUS Server, on page 256
- Login Settings, on page 262
- Login Protection Status, on page 265
- Key Management, on page 266
- Management Access Method, on page 268
- Management Access Authentication, on page 272
- Secure Sensitive Data Management, on page 273
- SSL Server, on page 276
- SSH Server, on page 278
- SSH Client, on page 281
- TCP/UDP Services, on page 284
- Storm Control, on page 285
- Port Security, on page 287
- 802.1X Authentication, on page 289
- Denial of Service Prevention, on page 298
- IP Source Guard, on page 304
- ARP Inspection, on page 306
- IPv6 First Hop Security, on page 309
- Certificate Settings, on page 325

TACACS+ Client

An organization can establish a Terminal Access Controller Access Control System (TACACS+) server to provide centralized security for all of its devices. In this way, authentication and authorization can be handled on a single server for all devices in the organization.

The device can act as a TACACS+ client that uses the TACACS+ server for the following services: The TACACS+ page enables configuring TACACS+ servers.

- Authentication—Provides authentication of users logging onto the device by using usernames and user-defined passwords.

- Authorization—Performed at login. After the authentication session is completed, an authorization session starts using the authenticated username. The TACACS+ server then checks user privileges.
- Accounting—Enable accounting of login sessions using the TACACS+ server. This enables a system administrator to generate accounting reports from the TACACS+ server.

TACACS+ is supported only with IPv4.

To configure TACACS+ server parameters, follow these steps:

Procedure

Step 1 Click **Security** > **TACACS+ Client**.

Step 2 Enable TACACS+ Accounting if required.

Step 3 Enter the following default parameters:

Option	Description
Key String	Enter the default Key String used for communicating with all TACACS+ servers in Encrypted or Plaintext mode. If you enter both a key string here and a key string for an individual TACACS+ server, the key string configured for the individual TACACS+ server takes precedence.
Timeout for Reply	Enter the amount of time that passes before the connection between the device and the TACACS+ server times out. If a value isn't entered in the Add TACACS+ Server page for a specific server, the value is taken from this field.
Source IPv4 Interface	Select the device IPv4 source interface to be used in messages sent for communication with the TACACS+ server.
Source IPv6 Interface	Select the device IPv6 source interface to be used in messages sent for communication with the TACACS+ server. **Note** If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

Step 4 Click **Apply**. The TACACS+ default settings are added to the Running Configuration file. These are used if the equivalent parameters are not defined in the Add page.

The information for each TACACS server is displayed in the TACACS+ Server Table. The fields in this table are entered in the Add page except for the Status field. This field describes whether the server is connected or not to the device.

Step 5 To add a TACACS+ server, click **Add.**

Step 6 Enter the parameters.

Option	Description
Server Definition	Select one of the following ways to identify the TACACS+ server: • By IP address-If this is selected, enter the IP address of the server in the Server IP Address/Name field.

Option	Description
	• By name-If this is selected enter the name of the server in the Server IP Address/Name field.
IP Version	Select the supported IP version of the source address: IPv6 or IPv4.
IPv6 Address Type	Select the IPv6 address type (if IPv6 is used). The options are: • Link Local-The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration. • Global-The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
Link Local Interface	Select the link local interface (if IPv6 Address Type Link Local is selected) from the list.
Server IP Address/Name	Enter the IP address or name of the TACACS+ server.
Priority	Enter the order in which this TACACS+ server is used. Zero is the highest priority TACACS+ server and is the first server used. If it can't establish a session with the high priority server, the device tries the next highest priority server.
Key String	Enter the default key string used for authenticating and encrypting between the device and the TACACS+ server. This key must match the key configured on the TACACS+ server. A key string is used to encrypt communications by using MD5. You can select the default key on the device, or the key can be entered in Encrypted or Plaintext form. If you don't have an encrypted key string (from another device), enter the key string in plaintext mode and click **Apply**. The encrypted key string is generated and displayed.
Timeout for Reply	Select **User Defined** and enter the amount of time that passes before the connection between the device and the TACACS+ server times out. Select **Use Default** to use the default value displayed on the page.
Authentication IP Port	Enter the port number through which the TACACS+ session occurs.
Single Connection	Select to enable receiving all information in a single connection. If the TACACS+ server doesn't support this, the device reverts to multiple connections.

Step 7 Click **Apply**. The TACACS+ server is added to the Running Configuration file of the device.

Step 8 To display sensitive data in plaintext form on this page, click **Display Sensitive Data As Plaintext**.

RADIUS Client

Remote Authorization Dial-In User Service (RADIUS) servers provide a centralized 802.1X or MAC-based network access control. The device can be configured to be a RADIUS client that can use a RADIUS server

to provide centralized security, and as a RADIUS server. An organization can use the device as establish a Remote Authorization Dial-In User Service (RADIUS) server to provide centralized 802.1X or MAC-based network access control for all of its devices. In this way, authentication and authorization can be handled on a single server for all devices in the organization.

Use RADIUS in network environments that require access security. To set the RADIUS server parameters, follow these steps:

Procedure

Step 1 Click **Security** > **RADIUS Client**.

Step 2 Enter the RADIUS Accounting option. The following options are available:

- Port Based Access Control (802 1X, MAC Based, Web Authentication)—Specifies that the RADIUS server is used for 802.1X port accounting.
- Management Access—Specifies that the RADIUS server is used for user login accounting.
- Both Port Based Access Control and Management Access—Specifies that the Radius server is used for both user login accounting and 802.1X port accounting.
- None—Specifies that the RADIUS server is not used for accounting.

Step 3 Enter the default RADIUS parameters if required. Values entered in the Default Parameters are applied to all servers. If a value is not entered for a specific server (in the Add RADIUS Server page) the device uses the values in these fields.

- Retries—Enter the number of transmitted requests that are sent to the RADIUS server before a failure is considered to have occurred.
- Timeout for Reply—Enter the number of seconds that the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server.
- Dead Time—Enter the number of minutes that elapse before a non-responsive RADIUS server is bypassed for service requests. If the value is 0, the server is not bypassed.
- Key String—Enter the default key string used for authenticating and encrypting between the device and the RADIUS server. This key must match the key configured on the RADIUS server. A key string is used to encrypt communications by using MD5. The key can be entered in Encrypted or Plaintext form. If you do not have an encrypted key string (from another device), enter the key string in plaintext mode and click Apply. The encrypted key string is generated and displayed.

This overrides the default key string if one has been defined.

- Source IPv4 Interface—Select the device IPv4 source interface to be used in messages for communication with the RADIUS server.
- Source IPv6 Interface—Select the device IPv6 source interface to be used in messages for communication with the RADIUS server.

Note
If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

Step 4 Click **Apply**. The RADIUS default settings for the device are updated in the Running Configuration file.

Step 5 To add a RADIUS server, click **Add**.

Step 6 Enter the values in the fields for each RADIUS server.

- Server Definition—Select whether to specify the RADIUS server by IP address or name.
- IP Version—Select the version of the IP address of the RADIUS server.
- IPv6 Address Type—Select the IPv6 address type (if IPv6 is used). The options are:
  - Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- Link Local Interface—Select the link local interface (if IPv6 Address Type Link Local is selected) from the list. •
- Server IP Address/Name—Enter the RADIUS server by IP address or name.
- Priority—Enter the priority of the server. The priority determines the order the device attempts to contact the servers to authenticate a user. The device starts with the highest priority RADIUS server first. Zero is the highest priority.
- Key String—Enter the key string used for authenticating and encrypting communication between the device and the RADIUS server. This key must match the key configured on the RADIUS server. It can be entered in Encrypted or Plaintext format. If Use Default is selected, the device attempts to authenticate to the RADIUS server by using the default Key String.
- Timeout for Reply—Select User Defined and enter the number of seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server if the maximum number of retries made. If Use Default is selected, the device uses the default timeout value.
- Authentication Port—Enter the UDP port number of the RADIUS server port for authentication requests
- Accounting Port—Enter the UDP port number of the RADIUS server port for accounting requests.
- Retries—Select User Defined and enter the number of requests that are sent to the RADIUS server before a failure is considered to have occurred. If Use Default is selected, the device uses the default value for the number of retries.
- Dead Time—Select User Defined and enter the number of minutes that must pass before a non-responsive RADIUS server is bypassed for service requests. If Use Default is selected, the device uses the default value for the dead time. If you enter 0 minutes, there is no dead time.
- Usage Type—Enter the RADIUS server authentication type. The options are:
  - Login—RADIUS server is used for authenticating users that ask to administer the device.
  - 802.1x—RADIUS server is used for 802.1x authentication.
  - All—RADIUS server is used for authenticating user that ask to administer the device and for 802.1X authentication.

Step 7 Click **Apply**. The RADIUS server definition is added to the Running Configuration file of the device.

Step 8 To display sensitive data in plaintext form on the page, click **Display Sensitive Data As Plaintext**.

RADIUS Server

An organization can use the device as a Remote Authorization Dial-In User Service (RADIUS) server to provide centralized 802.1X or MAC-based network access control for all of its devices. Thus, authentication and authorization can be handled on a single server for all devices.

When the device is configured as a RADIUS client, it can use the RADIUS server for the following services:

- Authentication-Provides authentication of regular and 802.1X users by using usernames and user-defined passwords
- Authorization-Performed at login After the authentication session is completed, an authorization session starts using the authenticated username. The RADIUS server then checks user privileges.

Accounting-Enable accounting of login sessions using the RADIUS server. This enables a system administrator to generate accounting reports from the RADIUS server. The user-configurable, TCP port used for RADIUS server accounting is the same TCP port that is used for RADIUS server authentication and authorization.

RADIUS Server Global Settings

The device can be configured as a RADIUS server. To set the RADIUS server global parameters, follow these steps:

Procedure

Step 1 Click **Security** > **RADIUS Server** > **RADIUS Server Global Settings**.

Step 2 Enter the following parameters:

- RADIUS Server Status—Check to enable the RADIUS server feature status.
- Authentication Port—Enter the UDP port number of the RADIUS server port for authentication requests.
- Accounting Port—Enter the UDP port number of the RADIUS server port for accounting requests.

Trap Settings

- RADIUS Accounting Traps—Check to generate traps for RADIUS accounting events.
- RADIUS Authentication Failure Traps—Check to generate traps for logins that failed.
- RADIUS Authentication Success Traps—Check to generate traps for logins that succeeded.

Step 3 Click **Apply**. The RADIUS default settings for the device are updated in the Running Configuration file.

RADIUS Server Keys

To set the RADIUS server keys, follow these steps:

Procedure

Step 1 Click **Security** > **RADIUS Server** > **RADIUS Server Keys**.

Step 2 Enter the default RADIUS keys if required. Values entered in the Default Key are applied to all servers configured (in the Add RADIUS Server page) to use the default key.

- Default Key—Enter the default key string used for authenticating and encrypting between the device and the RADIUS client. Select one of the following options:
  - Keep existing default key—For specified servers, the device attempts to authenticate the RADIUS client by using the existing, default Key String.
  - Encrypted—To encrypt communications by using MD5, enter the key in encrypted form.
  - Plaintext—Enter the key string in plaintext mode.
- MD5 Digest—Displays the MD5 digest of the user-entered password.

Step 3 Click **Apply**. The RADIUS default settings for the device are updated in the Running Configuration file.

Step 4 To add a secret key, click **Add** and enter the following fields:

- NAS Address—Address of switch containing RADIUS client.
- Secret Key—Address of switch containing RADIUS client.
  - Use default Key—For specified servers, the device attempts to authenticate the RADIUS client by using the existing, default Key String.
  - Encrypted—To encrypt communications by using MD5, enter the key in encrypted form.
  - Plaintext—Enter the key string in plaintext mode.

Step 5 Click **Apply**. The key for the device is updated in the Running Configuration file.

RADIUS Server Groups

To set up a group of users that will be using the device as its RADIUS server, complete the following:

Procedure

Step 1 Click **Security** > **RADIUS Server** > **RADIUS Server Groups**.

Step 2 Click **Add** and enter the following fields:

- Group Name—Enter a name for the group.
- Privilege Level—Enter the management access privilege level of the group.
- Time Range—Check to enable applying a time range to this group.

- Time Range Name—If Time Range is selected, select the time range to be used. Click **Edit** to define a time range. This field is only displayed if a Time Range was previously created.
- VLAN—Select the VLAN for the users:
  - None—No VLAN ID is sent.
  - VLAN ID—VLAN ID sent.
  - VLAN Name—VLAN name sent

Step 3 Click **Apply**. The RADIUS group definition is added to the Running Configuration file of the device.

RADIUS Server Users

To add a user, follow these steps:

Procedure

Step 1 Click **Security** > **RADIUS Server** > **RADIUS Server Users**.

The current users are displayed.

Step 2 Click **Add** to add a RADIUS Server User or **Edit** to edit an existing one. Next, complete the following:

- User Name—Enter the name of a user.
- Group Name—Select a previously defined group.
- Password MD5—a cryptographic hash algorithm of the password will be displayed. (Only available in Edit mode).
- Password—Enter one of the following options:
  - Keep current password—Select to keep current password. (Only available in Edit mode).
  - Encrypted—A key string is used to encrypt communications by using MD5. To use encryption, enter the key in encrypted form.
  - Plaintext—If you don't have an encrypted key string (from another device), enter the key string in plaintext mode. The encrypted key string is generated and displayed.

Step 3 Click **Apply**. The user definition is added to the Running Configuration file of the device.

RADIUS Server Accounting

The Radius server saves the last accounting logs in a cycle file on FLASH. These can be displayed.

To display RADIUS server accounting, complete the following steps:

Procedure

Step 1 Click **Security** > **RADIUS Server** > **RADIUS Server Accounting**.

RADIUS accounting events are displayed along with the following fields:

- User Name—Name of a user.
- Event Type—One of the following values:
  - Start—Session was started.
  - Stop—Session was stopped.
  - Date/Time Change—Date/time on the device was changed.
  - Reset—Device has reset at the specified time.
- Authentication Method—Authentication method used by the user. Displays N/A if the Event Type is Date/Time Change or Reset.
- NAS Address—Address of switch containing RADIUS client. Displays N/A if the Event Type is Date/Time Change or Reset.
- User Address—If the authenticated user is the network administrator, this is its IP address; if the user is a station, this is its MAC address. Displays N/A if the Event Type is Date/Time Change or Reset.
- Event Time—Time of event.

Step 2 To see additional details for a user/event, select the user/event and click **Details**.

The following fields are displayed:

Note The fields in this page depend on the type of account viewed and the details received for it. Not all fields are always displayed.

- Event Time—See above.
- Event Type—See above.
- User Name—See above.
- Authentication Method—See above.
- NAS IPv4 Address—See NAS Address above.
- NAS Port—Port used on the switch at the NAS address
- User Address—See above.
- Accounting Session Time—See Event Time above.
- Session Termination Reason—Displays reason for session termination, such as User Request.

RADIUS Server Rejected Users

To view the users who have attempted to authenticate using the RADIUS server and have been rejected, complete the following steps:

Procedure

Step 1 Click **Security** > **RADIUS Server** > **RADIUS Rejected Users**.

The rejected users are displayed along with the following fields:

- Event Type—Displays one of the following options:
  - Rejected—User was rejected.
  - Time Change—Clock on device was changed by the administrator.
  - Reset—Device was reset by the administrator.
- User Name—Name of the rejected user.
- User Type—Displays one of the following authentication options relevant to the user:
  - Login—Management access user
  - 802.1x—802.1x network access user
  - N/A—For Reset event
- Reason—Reason that the user was rejected.
- Time—Time that the user was rejected.

Step 2 To see additional details for the rejected user, select the user and click **Details**.

The following fields are displayed:

Note The fields in this page depend on the type of account viewed and the details received for it. Not all fields are always displayed.

- Event Time—See above.
- User Name—See above.
- User Type—See above.
- Rejection Reason—Reason that the user was rejected.
- NAS IP Address—Address of the Network Accessed Server (NAS). The NAS is the switch running the RADIUS client.

To clear out the table of rejected users, click **Clear**.

RADIUS Server Unknown NAS Entries

To display authentication rejections due to NASs not being known to RADIUS server, complete the following:

Procedure

Step 1 Click **Security** > **RADIUS Server** > **RADIUS Server Unknown NAS Entries**.

The following fields are displayed:

- Event Type
  - Unknown NAS—An unknown NAS event occurred.
  - Time Change—Clock on device was changed by the administrator.
  - Reset—Device was reset by the administrator.
- IP Address—IP address of the unknown NAS.
- Time—Timestamp of event

Step 2 Click **Clear** to delete an entry.

RADIUS Server Statistics

To display RADIUS server statistics, follow these steps:

Procedure

Step 1 Click **Security** > **RADIUS Server** > **RADIUS Server Statistics**.

Step 2 Select the Statistics Source from the following options:

- • Global—Statistics for all users
  - Specific NAS—Statistics for specific NAS

Step 3 Select the Refresh Rate.

Step 4 The following statistics will be displayed.

Incoming Packets on Authentication Port	Number of packets received on the authentication port.
Incoming Access-Requests from Unknown Addresses	Number of incoming access requests from unknown NAS addresses
Duplicate Incoming Access-Requests	Number of retransmitted packets received.
Sent Access-Accepts	Number of access accepts sent.

Sent Access-Rejects	Number of access rejects sent.
Sent Access-Challenges	Number of access challenges sent.
Incoming Malformed Access-Requests	Number of malformed access requests received.
Incoming Authentication-Requests with Bad Authenticator	Number of incoming packets with bad passwords.
Incoming Authentication Packets with Other Mistakes	Number of received incoming authentication packets with other mistakes.
Incoming Authentication Packets of Unknown Type	Number of received incoming authentication packets of unknown type
Incoming Packets on the Accounting Port	Number of incoming packets on the accounting port.
Incoming Authentication-Requests from Unknown Addresses	Number of incoming authentication requests from unknown addresses.
Incoming Duplicate Accounting-Requests	Number of incoming duplicate account requests.
Accounting-Responses Sent	Number of accounting responses sent.
Incoming Malformed Accounting-Requests	Number of malformed accounting requests.
Incoming Accounting-Requests with Bad Authenticator	Number of incoming accounting requests with bad authenticator.
Incoming Accounting Packets with Other Mistakes	Number of incoming accounting packets with other mistakes.
Incoming Not Recorded Accounting-Requests	Number of incoming accounting requests not recorded.
Incoming Accounting Packets of Unknown Type	Number of incoming accounting packets of unknown type.

Step 5 To clear the counters, click **Clear Counters**.

Step 6 To refresh the counters, click **Refresh**.

Login Settings

The default username/password is **cisco/cisco**. The first time that you log in with the default username and password, you're required to enter a new password. Password complexity is enabled by default. If the password that you choose isn't complex enough, then you will be prompted to create another password.

Procedure

Step 1 Click **Security** > **Login Settings** .

Step 2 In the Password Aging section, check **Enable** to enable the password aging. When the Password Aging checkbox is unchecked, the Password Aging Time is disabled.

Step 3 Next, configure the following:

Option	Description
Password Aging Time	Enter the number of days. (Range: 1 - 365, Default: 180) **Note** A warning message will appear 10 days prior to the password expiration date. From the expiration day and on, the user logging in will be forced to change the password and will not be granted access to the device until the password is changed.
Recent Password Prevention	Check **Enable** to enable this feature. It is disabled by default.
Password History Count	Defines the number for a recent password prevention. range is 1- 24 and default is 12.
Minimal Password Length	Enter the number of character for the password. (Range: 8-64, Default: 8)
Allowed Character Repetition	A character cannot be repeated consecutively. Enter a number for the allowed character repetition. (Range: 1- 16, Default: 3)
Minimal Number of Character Classes:	Enter a number for the minimal number of character classes. (Range: 0- 4, Default: 3)

Note
The password complexity rules are as follows:

- Minimal password length is 8 characters by default. Passwords are configurable with a range of 8-64.
- Character Repetition: A character cannot be repeated consecutively. The minimum number of repetition allowed is 3 by default.
- Recent password prevention: The password must be different than a number of previously used passwords on this account. 12 by default, configurable to 3-24.
- Minimum number of character classes: The number of different character classes that must be included in the password (classes are: uppercase letter, lowercase letter, number and special character). The minimum number is 3 by default and is configurable to 0-4 (0 and 1 are functionally identical).
- Any password established or altered by the user (hence "Secret") must be compared to the following file's list of common passwords. If the secret contains a word from the list, the user will receive the following error message and will need to re-enter an alternative password: "Password rejected- Passwords must not match words in the dictionary, and must not contain commonly used passwords".

Definition for Known Password

When a user attempts to configure a new password, it is compared against the list of commonly used passwords. If new password contains one of the passwords in the common password list the user configuration is rejected and the user will need to configure a different password.

The new password is considered to contain a “word” (common password) in the list, if:

a. The word appears in any part of the password (beginning, middle, or end).

b. The word appears in reverse order in the password.

c. The word appears in the password in any case (lower or upper case) combination

d. The word letters are replaced with other characters, as follows: "$" for "s", "@" for "a", "0" for "o", "1" for "l", "!" for "i", "3" for "e", is not permitted. For example, Pa$$w0rd is not permitted.

Definition for Sequential Characters

The password MUST NOT contain more than 2 sequential characters or numbers, or the reverse value of these sequences. Restriction also includes letters that are replaced with other characters, as follows: "$" for "s", "@" for "a", "0" for "o", "1" for "l", "!" for "i", "3" for "e".

Examples for prohibited passwords: “efg123!$”, “abcd765%”, “kji!$378”, qr$58!230.

Sequential letters are prohibited in any case combination (e.g. AbC or aBC).

If the password does not comply to these rules the configuration will be rejected and the user will need to configure a new password.

Login Lockdown

If the address of a device is known, a malicious user may attempt to perform a dictionary attack. A dictionary attack is an automated process to attempt to login by attempting thousands, or even millions, of credentials. The purpose of a dictionary attack is to actually gain management access to the device.

To prevent these attacks the device can be configured to limit the amount of login attempts allowed within a specific time range and by defining a quiet mode period following a specified number of failed attempts. If the specified number of connection attempts fails (attempt tries) within a specified time (within seconds), the device will not accept any additional login attempts for a specified period of time (block-for seconds). This can also occur when the user forgets his login credentials and tries to login several times resulting in login failure.



Note Following a specified number of failed login attempts over a specified time period, the device will enter into quiet mode. The device will not accept any more connection requests during the quiet mode time, including telnet, SSH, SNMP, HTTP, or HTTPS. The device will restart accepting connection requests once the quiet mode period has ended. The start and conclusion of the quiet mode time will be indicated by a Syslog message.

The number of failed attempts should be counted throughout a period of time that is measured from each failed attempt. Failed attempts are not counted during the quiet period. When the quiet period expires, the count of failed attempts resumes. A quiet period can be ended before the timer expires by disabling the functionality.

Procedure

Step 1 In the Login Response Delay, check **Enable** to enable the login response delay.

Step 2 Next, configure the following:

Option	Description
Response Delay Period	Enter a number in seconds to set the response delay period. (Range: 1- 10, Default: 1)
Quiet Period Enforcement	Check **Enable** to enforce quite period.
Quiet Period Length	Enter the number of seconds to set the quiet period length. (Range: 1- 65535, Default: 300)
Triggering Attempts	Enter the number of triggering attempts. (Range: 1- 100, Default: 4)
Triggering Interval	Enter the number in seconds for triggering interval. (Range: 1- 3600, Default: 60)
Quiet PeriodAccess Profiles, on page 269. **Note** This link navigates to the Security → Management Access Method → Access Profiles page.	Console Only is the default setting. **Note** This drop down contains an option for every existing access profile.

Login Protection Status

The Login Protection Status page will track and display any attempted attacks or login failures. (It will not distinguish if the login failure is a user who forgot his credentials or an actual attack). Click the **Refresh** button to refresh the data.

To view the settings for the Login Protection Status, navigate to **Security > Login Protection Status.**

- Quiet Mode Status- Can have either an active or inactive status.
- Login Failures in the Last 0 Seconds- Displays the number of login failures during the time lapse defined by the "Quiet Period Length" Parameter. The "Quiet Period Length" is a value in seconds configured in the **Security > Login Settings** page.

In the Login Failure Table, the following will be displayed:

- Username- the name of the user
- IP Address- the IP address of the user
- Service- the service being used. This can be either HTTP, HTTPS, Telnet, SSH or SNMP.

- Count- the number of attempted login failures.
- Most Recent Attempt Time- the most recent time that a failed login was attempted.

Key Management

This section describes how to configure key chains for applications and protocols, such as RIP.

Key Chain

To create a new key chain.

Procedure

Step 1 Click **Security** > **Key Management** > **Key Chain Settings**.

Step 2 To add a new key chain, click **Add** to open the Add Key Chain page and enter the following fields:

- Key Chain-Name for the key chain.
- Key Identifier-Integer identifier for the key chain.
- Key String-Value of the key chain string. Enter one of the following options:
  - User Defined (Encrypted)-Enter an encrypted version.
  - User Defined (Plaintext)-Enter a plaintext version

  Note
  Both the Accept Life Time and the Send LifeTime values can be entered. The Accept Life Time indicates when the key-identifier for receiving packets is valid. The Send Life Time indicates when the key-identifier for sending packets is valid.

- Accept Life Time/Send Life Time-Specifies when packets with this key are accepted. Select one of the following options.
  - Always Valid-No limit to the life of the key-identifier
  - User Defined-Life of the key-chain is limited. If this option, is selected enter values in the following fields.

  Note
  If you select User Defined, the system time must be set either manually or from SNTP. Otherwise, Accept Life Time and Send Life Times always fail.

  The following fields are relevant for the Accept Life Time and Send Life Time fields:

- Start Date-Enter the earliest date that the key-identifier is valid.
- Start Time-Enter the earliest time that the key-identifier is valid on the Start Date.
- End Time-Specifies the last date that the key-identifier is valid. Select one of the following options.
  - Infinite-No limit to the life of the key-identifier

- Duration-Life of the key-identifier is limited. If this option, is selected enter values in the following fields.

- Duration-Length of time that the key identifier is valid. Enter the following fields:
  - Days-Number of days that the key-identifier is valid.
  - Hours-Number of hours that the key-identifier is valid.
  - Minutes-Number of minutes that the key-identifier is valid.
  - Seconds-Number of seconds that the key-identifier is valid.

Step 3 Click **Apply**. The settings are written to the Running Configuration file.

Key Settings

To add a key to an already existing key chain.

Procedure

Step 1 Click **Security** > **Key Management** > **Key Settings**.

Step 2 Click **Add** to add a key string or **Edit** to edit and existing one.

Step 3 Enter the following fields:

- Key Chain-Name for the key chain.
- Key Identifier-Integer identifier for the key chain.
- Key String-Value of the key chain string. Enter one of the following options:
  - User Defined (Encrypted)-Enter an encrypted version.
  - User Defined (Plaintext)-Enter a plaintext version.

  Note
  Both the Accept Life Time and the Send LifeTime values can be entered. The Accept Life Time indicates when the key-identifier for receiving packets is valid. The Send Life Time indicates when the key-chain for sending packets is valid. The fields are only described for the Accept Life Time. The Send Life Time has the same fields.

- Accept Life Time-Specifies when packets with this key are accepted. Select one of the following options.
  - Always Valid-No limit to the life of the key-identifier
  - User Defined-Life of the key-chain is limited. If this option, is selected enter values in the following fields.

- Start Date-Enter the earliest date that the key-identifier is valid.
- Start Time-Enter the earliest time that the key-identifier is valid on the Start Date.
- End Time-Specifies the latest time that the key-identifier is valid. Select one of the following options.

- Infinite-No limit to the life of the key-identifier
- Duration-Life of the key-identifier is limited. If this option, is selected enter values in the following fields.

- Duration-Length of time that the key identifier is valid. Enter the following fields:
  - Days-Number of days that the key-identifier is valid.
  - Hours-Number of hours that the key-identifier is valid.
  - Minutes-Number of minutes that the key-identifier is valid.
  - Seconds-Number of seconds that the key-identifier is valid.

Step 4 Click **Apply**. The settings are written to the Running Configuration file.

Step 5 Click **Details** to view the key details or click **Display Sensitive Data as Plaintext** to display the sensitive data as plaintext (and not in encrypted form),

Management Access Method

This section describes access rules for various management methods.

Access profiles determine how to authenticate and authorize users accessing the device through various access methods. Access Profiles can limit management access from specific sources.

Only users who pass both the active access profile and the management access authentication methods are given management access to the device.

There can only be a single access profile active on the device at one time.

Access profiles consist of one or more rules. The rules are executed in order of their priority within the access profile (top to bottom).

Rules are composed of filters that include the following elements:

- Access Methods-Methods for accessing and managing the device:
  - Telnet
  - Secure Telnet (SSH)
  - Hypertext Transfer Protocol (HTTP)
  - Secure HTTP (HTTPS)
  - Simple Network Management Protocol (SNMP)
  - All of the above
- Action-Permit or deny access to an interface or source address.
- Interface-Which ports, LAGs, or VLANs are permitted to access or are denied access to the web-based configuration utility.

- Source IP Address-IP addresses or subnets. Access to management methods might differ among user groups. For example, one user group might be able to access the device module only by using an HTTPS session, while another user group might be able to access the device module by using both HTTPS and Telnet sessions.

Access Profiles

The Access Profiles page displays the access profiles that are defined and enables selecting one access profile to be the active one.

When a user attempts to access the device through an access method, the device looks to see if the active access profile explicitly permits management access to the device through this method. If no match is found, access is denied.

When an attempt to access the device is in violation of the active access profile, the device generates a SYSLOG message to alert the system administrator of the attempt.

If a console-only access profile has been activated, the only way to deactivate it's through a direct connection from the management station to the physical console port on the device.

For more information, see Profile Rules, on page 270.

Use the Access Profiles page to create an access profile and to add its first rule. If the access profile only contains a single rule, you're finished. To add more rules to the profile, use the Profile Rules page.

Procedure

Step 1 Click **Security** > **Mgmt Access Method** > **Access Profiles**.

This page displays all of the access profiles, active and inactive.

Step 2 To change the active access profile, select a profile from the Active Access Profile drop down menu and click **Apply**. This makes the chosen profile the active access profile.

Note
A caution message appears if you selected Console Only. If you continue, you're immediately disconnected from the web-based configuration utility and can access the device only through the console port. This only applies to device types that offer a console port.

Step 3 Click **OK** to select the active access profile or click **Cancel** to discontinue the action.

Step 4 Click **Add** to open the Add Access Profile page. The page allows you to configure a new profile and one rule.

Step 5 Enter the Access Profile Name. This name can contain up to 32 characters.

Step 6 Enter the parameters.

- Rule Priority—Enter the rule priority. When the packet is matched to a rule, user groups are either granted or denied access to the device. The rule priority is essential to matching packets to rules, as packets are matched on a first-match basis. The highest priority is '1'.
- Management Method—Select the management method for which the rule is defined. The options are:
  - All—Assigns all management methods to the rule

- Telnet—Users requesting access to the device that meets the Telnet access profile criteria are permitted or denied access.
- Secure Telnet (SSH)—Users requesting access to the device that meets the SSH access profile criteria, are permitted or denied access.
- HTTP— Users requesting access to the device that meets the HTTP access profile criteria, are permitted or denied.
- Secure HTTP (HTTPS)—Users requesting access to the device that meets the HTTPS access profile criteria, are permitted or denied.
- SNMP—Users requesting access to the device that meets the SNMP access profile criteria are permitted or denied.

- Action—Select the action attached to the rule. The options are:
  - Permit—Permits access to the device if the user matches the settings in the profile.
  - Deny—Denies access to the device if the user matches the settings in the profile
- Applies to Interface—Select the interface attached to the rule. The options are:
  - All—Applies to all ports, VLANs, and LAGs
  - User Defined—Applies to selected interface.
- Interface—Enter the interface number if User Defined was selected.
- Applies to Source IP Address—Select the type of source IP address to which the access profile applies. The Source IP Address field is valid for a subnetwork. Select one of the following values:
  - All—Applies to all types of IP addresses
  - User Defined—Applies to only those types of IP addresses defined in the fields.
- IP Version—Enter the version of the source IP address: Version 6 or Version 4.
- IP Address—Enter the source IP address.
- Mask—Select the format for the subnet mask for the source IP address, and enter a value in one of the fields:
  - Network Mask—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
  - Prefix Length—Select the Prefix Length and enter the number of bits that comprise the source IP address prefix.

Step 7 Click **Apply**. The access profile is written to the Running Configuration file. You can now select this access profile as the active access profile.

Profile Rules

Access profiles can contain up to 128 rules to determine who is permitted to manage and access the device, and the access methods that may be used.

Each rule in an access profile contains an action and criteria (one or more parameters) to match. Each rule has a priority; rules with the lowest priority are checked first. If the incoming packet matches a rule, the action associated with the rule is performed. If no matching rule is found within the active access profile, the packet is dropped.

For example, you can limit access to the device from all IP addresses except IP addresses that are allocated to the IT management center. In this way, the device can still be managed and has gained another layer of security.

To add profile rules to an access profile, complete the following steps:

Procedure

Step 1 Click **Security > Mgmt Access Method > Profile Rules**.

Step 2 Select the Filter field, and an access profile. Click **Go**.

The selected access profile appears in the Profile Rule Table.

Step 3 Click **Add** to add a rule.

Step 4 Enter the parameters.

- Access Profile Name—Select an access profile.
- Rule Priority—Enter the rule priority. When the packet is matched to a rule, user groups are either granted or denied access to the device. The rule priority is essential to matching packets to rules, as packets are matched on a first-fit basis.
- Management Method—Select the management method for which the rule is defined. The options are:
  - All—Assigns all management methods to the rule
  - Telnet—Users requesting access to the device that meets the Telnet access profile criteria are permitted or denied access.
  - Secure Telnet (SSH)—Users requesting access to the device that meets the Telnet access profile criteria, are permitted or denied access.
  - HTTP—Assigns HTTP access to the rule Users requesting access to the device that meets the HTTP access profile criteria, are permitted or denied.
  - Secure HTTP (HTTPS)—Users requesting access to the device that meets the HTTPS access profile criteria, are permitted or denied.
  - SNMP—Users requesting access to the device that meets the SNMP access profile criteria are permitted or denied.
- Action—Select one of the following options.
  - Permit—Allow device access to users coming from the interface and IP source defined in this rule.
  - Deny—Deny device access to users coming from the interface and IP source defined in this rule.
- Applies to Interface—Select the interface attached to the rule. The options are:
  - All—Applies to all ports, VLANs, and LAGs

- User Defined—Applies only to the port, VLAN, or LAG selected.

- Interface—Enter the interface number if the User Defined option is selected for the field above.
- Applies to Source IP Address—Select the type of source IP address to which the access profile applies. The Source IP Address field is valid for a subnetwork. Select one of the following values:
  - All—Applies to all types of IP addresses
  - User Defined—Applies to only those types of IP addresses defined in the fields.
- IP Version—Select the supported IP version of the source address: IPv6 or IPv4.
- IP Address—Enter the source IP address.
- Mask—Select the format for the subnet mask for the source IP address, and enter a value in one of the fields:
  - Network Mask—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
  - Prefix Length—Select the Prefix Length and enter the number of bits that comprise the source IP address prefix.

Step 5 Click **Apply,** and the rule is added to the access profile.

Management Access Authentication

You can assign authentication methods to the various management access methods, such as SSH, Telnet, HTTP, and HTTPS. The authentication can be performed locally or on a server.

If authorization is enabled, both the identity and read/write privileges of the user are verified. If authorization isn't enabled, only the identity of the user is verified.

The authorization/authentication method used is determined by the order that the authentication methods are selected. If the first authentication method isn't available, the next selected method is used. For example, if the selected authentication methods are RADIUS and Local, and all configured RADIUS servers are queried in priority order and don't reply, the user is authorized/authenticated locally.

If authorization is enabled, and an authentication method fails or the user has insufficient privilege level, the user is denied access to the device. In other words, if authentication fails for an authentication method, the device stops the authentication attempt; it doesn't continue and doesn't attempt to use the next authentication method.

Similarly, if authorization isn't enabled, and authentication fails for a method, the device stops the authentication attempt.

To define authentication methods for an access method:

Procedure

Step 1 Click **Security** > **Management Access Authentication**.

Step 2 Enter the Application (type) of the management access method.

Step 3 Select **Authorization** to enable both authentication and authorization of the user by the list of methods described below. If the field is not selected, only authentication is performed. If Authorization is enabled, the read/write privileges of users are checked. This privilege level is set in the User Accounts page.

Step 4 Use the arrows to move the authentication method between the Optional Methods column and the Selected Methods column. The first method selected is the first method that is used.

- RADIUS—User is authorized/authenticated on a RADIUS server. You must have configured one or more RADIUS servers. For the RADIUS server to grant access to the web-based configuration utility, the RADIUS server must return RADIUS Attribute "Service-Type 6" value "Administrative".
- TACACS+—User authorized/authenticated on the TACACS+ server. You must have configured one or more TACACS+ servers.
- None—User is allowed to access the device without authorization/authentication.
- Local—Username and password are checked against the data stored on the local device. These username and password pairs are defined in the User Accounts page.

Note
The Local or None authentication method must always be selected last. All authentication methods selected after Local or None are ignored.

Step 5 Click **Apply**. The selected authentication methods are associated with the access method.

Secure Sensitive Data Management

SSD protects sensitive data on a device, such as passwords and keys, permits and denies access to sensitive data encrypted and in plain text based on user credentials and SSD rules, and protects configuration files containing sensitive data from being tampered with.

In addition, SSD enables the secure backup and sharing of configuration files containing sensitive data.

SSD provides users with the flexibility to configure the desired level of protection on their sensitive data; from no protection with sensitive data in plaintext, minimum protection with encryption based on the default passphrase, and better protection with encryption based on user-defined passphrase.

SSD grants read permission to sensitive data only to authenticated and authorized users, and according to SSD rules. A device authenticates and authorizes management access to users through the user authentication process.

Whether or not SSD is used, it is recommended that the administrator secure the authentication process by using the local authentication database, and/or secure the communication to the external authentication servers used in the user authentication process.

In summary, SSD protects sensitive data on a device with SSD rules, SSD properties, and user authentication. And SSD rules, SSD properties, and user authentication configurations of the device are themselves sensitive data protected by SSD.

SSD Properties

SSD properties are a set of parameters that, in conjunction with the SSD rules, define and control the SSD environment of a device. The SSD environment consists of these properties:

- Controlling how the sensitive data is encrypted.
- Controlling the strength of security on configuration files.
- Controlling how the sensitive data is viewed within the current session.

To configure the SSD properties, follow these steps:

Procedure

Step 1 Click **Security** > **Secure Sensitive Data Management** > **Properties**.

The following field appears:

- Current Local Passphrase Type—Displays whether the default passphrase or a user-defined passphrase is currently being used.

Step 2 In the Configuration File Passphrase Control—Select an option from the following:

- Unrestricted (default)—The device includes its passphrase when creating a configuration file. This enables any device accepting the configuration file to learn the passphrase from the file.
- Restricted—The device restricts its passphrase from being exported into a configuration file. Restricted mode protects the encrypted sensitive data in a configuration file from devices that do not have the passphrase. This mode should be used when a user does not want to expose the passphrase in a configuration file.

Step 3 Next, select to enable the Configuration File Integrity Control.

Step 4 Select a Read Mode for the current session

- Plaintext —Users are permitted to access sensitive data in plaintext only. Users will also have read and write permission to SSD parameters.
- Encrypted —Users are permitted to access sensitive data as encrypted only.

Step 5 Click **Change Local Passphrase**, and enter a new Local Passphrase:

- Default—Use the devices default passphrase.
- User Defined (Plaintext)—Enter a new passphrase.
- Confirm Passphrase—Confirm the new passphrase.

Step 6 Click **Apply**. The settings are saved to the Running Configuration file.

SSD Rules

Only users with SSD read permission of Plaintext-only or Both are allowed to set SSD rules.

To configure SSD rules, follow these steps:

Procedure

Step 1 Click **Security** > **Secure Sensitive Data Management** > **SSD Rules**.

The currently-defined rules are displayed. The Rule Type field indicates whether the rule is a user-defined one or a default rule.

Step 2 To add a new rule, click **Add**. Enter the following fields:

- User—This defines the user(s) to which the rule applies: Select one of the following options:
  - Specific User—Select and enter the specific user name to which this rule applies (this user does not necessarily have to be defined).
  - Default User (cisco)—Indicates that this rule applies to the default user.
  - Level 15—Indicates that this rule applies to all users with privilege level 15.
  - All—Indicates that this rule applies to all users.
- Channel—This defines the security level of the input channel to which the rule applies: Select one of the following options:
  - Secure—Indicates that this rule applies only to secure channels (console, SCP, SSH and HTTPS), not including the SNMP and XML channels.
  - Insecure—Indicates that this rule applies only to insecure channels (Telnet, TFTP and HTTP), not including the SNMP and XML channels.
  - Secure XML SNMP—Indicates that this rule applies only to XML over HTTPS and SNMPv3 with privacy.
  - Insecure XML SNMP—Indicates that this rule applies only to XML over HTTP or and SNMPv1/v2and SNMPv3 without privacy.
- Read Permission—The read permissions associated with the rule. These can be the following:
  - Exclude—Lowest read permission. Users are not permitted to get sensitive data in any form.
  - Plaintext Only—Higher read permission than above ones. Users are permitted to get sensitive data in plaintext only.
  - Encrypted Only—Middle read permission. Users are permitted to get sensitive data as encrypted only.
  - Both (Plaintext and Encrypted)—Highest read permission. Users have both encrypted and plaintext permissions and are permitted to get sensitive data as encrypted and in plaintext
- Default Read Mode—All default read modes are subjected to the read permission of the rule. The following options exist, but some might be rejected, depending on the rule's read permission.
  - Exclude—Do not allow reading the sensitive data.

- Encrypted—Sensitive data is presented encrypted.
- Plaintext—Sensitive data is presented as plaintext.

Step 3 Click **Apply**. The settings are saved to the Running Configuration file.

Step 4 The following actions can be performed on selected rules:

- Add, Edit or Delete rules or Restore To Default.
- Restore All Rules to Default—Restore a user-modified default rule to the default rule.

SSL Server

The Secure Socket Layer (SSL) feature is used to open an HTTPS session to the device. An HTTPS session may be opened with the default certificate that exists on the device. Some browsers generate warnings when using a default certificate, since this certificate is not signed by a Certification Authority (CA). It is best practice to have a certificate signed by a trusted CA. By default, the device contains certificates that can be modified. HTTPS is enabled by default.

SSL Server Authentication Settings

Secure Sockets Layer (SSL) authentication is a protocol for creating a secure connection for user-server interactions. A server and a user are involved in every web interaction. Users frequently enter sensitive, personal information on websites, putting persons and systems at risk. Better authentication strengthens security, especially for sites that store financial, medical, or personal data. Stable, verifiable, and secure user interactions are required. The way that a server verifies that the user is a real person is by collecting information. There are a number of ways this can be done.

Procedure

Step 1 Click **Security** > **SSL Server** > **SSL Server Authentication Settings.**

Step 2 The device includes 2 certificates. Only one of them is the active certificate which can be used for the HTTPS session. To define which certificate is active, in the SSL Active Certificate Number, select an active certificate (**1** or **2**).

Step 3 Click **Apply**.

Step 4 In the HTTPS Session Logging section, check **Enable** to enable. By enabling the HTTPS session logging, this will allow a user to track the progress of HTTPS session setup and tear-down, via syslog messages generated by the device.

Step 5 Click **Apply**.

Create or Generate a New Certificate

A new self-signed certificate maybe required to replace the certificate found on the device. To create a new certificate, complete the following steps:

Procedure

Step 1 Select a certificate and click **Edit**.

Step 2 Enter the following fields:

- Certificate ID—Select the certificate ID that is to be replaced.
- Regenerate RSA Key—Check the checkbox to regenerate a RSA key.
- Key Length—Select the key length from one of the 2 options (2048 bits or 3072 bits).
- Common Name—Specifies the fully-qualified device URL or IP address. If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).
- Organization Unit—Specifies the organization-unit or department name.
- Organization Name—Specifies the organization name.
- Location—Specifies the location or city name.
- State—Specifies the state or province name.
- Country—Specifies the country name.
- Duration—Define the duration of the certificate.

Step 3 Click **Generate**. The new certificate is generated and replaces existing one.

Step 4 If you wish to generate a new certificate request, select a certificate and click **Generate Certificate Request**.

Note
A certificate request is a certificate that is exported to a CA for signing, and then imported back to the device as a signed certificate. A certificate signed by a CA is considered secure (compare to a self sign certificate which is not).

Step 5 Enter the following fields:

- Certificate ID—Select the certificate ID that is to be replaced.
- Common Name—Specifies the fully-qualified device URL or IP address. If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).
- Organization Unit—Specifies the organization-unit or department name.
- Organization Name—Specifies the organization name.
- Location—Specifies the location or city name.
- State—Specifies the state or province name.
- Country—Specifies the country name.
- Certificate Request—Displays the key created when the Generate Certificate Request button is pressed.

Step 6 Click **Generate Certificate Request.** This creates a certificate that must be entered on the Certification Authority (CA). Copy the certificate key from the Certificate Request field.

Step 7 To import a certificate signed by a CA, select an active certificate and click **Import Certificate**.

Step 8 Enter the following fields:

- Certificate ID—Select a certificate.
- Certificate Source—Displays that the certificate is auto-generated.
- Certificate—Copy in the received certificate.
- Import RSA Key—Pair-Select to enable copying in the new RSA key-pair.
- Public Key—Copy in the RSA public key.
- Fingerprint(Hex)- Displays the certificate's fingerprint in Hex format.
- Private Key (Encrypted)—Select and copy in the RSA private key in encrypted form.
- Private Key (Plaintext)—Select and copy in the RSA private key in plain text form.

Step 9 Click **Apply** to apply the changes to the Running Configuration.

Step 10 Click the **Details** button to display the SSL certificate details.

Step 11 Next, click **Display Sensitive Data as Encrypted** to display this key as encrypted. When this button is clicked, the private keys are written to the configuration file in encrypted form (when **Apply** is clicked). When the text is displayed in encrypted form, the button becomes Display Sensitive Data as Plaintext enabling you to view the text in plaintext again.

SSH Server

The SSH Server feature enables a remote users to establish SSH sessions to the device. This is similar to establishing a telnet session, except the session is secured.

The device, as a SSH server, supports SSH User Authentication which authenticates a remote user either by password, or by public key. At the same time, the remote user as a SSH client can perform SSH Server Authentication to authenticate the device using the device public key (fingerprint).

SSH Server can operate in the following modes:

- By Internally-generated RSA/DSA Keys (Default Setting)—An RSA and a DSA key are generated. Users log on the SSH Server application and are automatically authenticated to open a session on the device when they supply the IP address of the device.
- Public Key Mode—Users are defined on the device. Their RSA/DSA keys are generated in an external SSH server application, such as PuTTY. The public keys are entered in the device. The users can then open an SSH session on the device through the external SSH server application.

SSH User Authentication

If you use the SSH User Authentication page to create an SSH username for a user who is already configured in the local user database. You can prevent additional authentication by configuring the Automatic Login feature, which works as follows:

- Enabled—If a user is defined in the local database, and this user passed SSH Authentication using a public-key, the authentication by the local database username and password is skipped.

Note The configured authentication method for this specific management method (console, Telnet, SSH and so on) must be Local (i.e. not RADIUS or TACACS+).

- Not Enabled—After successful authentication by SSH public key, even if the username is configured in the local user database, the user is authenticated again, as per the configured authentication methods.

This feature is optional and can be configured on the Management Access Authentication, on page 272. You do not have to work with user authentication in SSH.

To enable authentication and add a user.

Procedure

Step 1 Click **Security** > **SSH Server** > **SSH User Authentication**.

Step 2 Select the following fields:

- SSH User Authentication by Password—Select to perform authentication of the SSH client user using the username/password configured in the local database (see User Accounts, on page 62).
- SSH Session Logging— Click **Enable** to enable SSH session logging. The SSH session logging allows a user to track the progress of an SSH session setup and tear-down, via syslog messages generated by the device.
- SSH User Authentication by Public Key—Select to perform authentication of the SSH client user using the public key.
- Automatic Login—This field can be enabled if the SSH User Authentication by Public Key feature was selected.

Step 3 Click **Apply**. The settings are saved to the Running Configuration file.

The following fields are displayed for the configured users:

- SSH User Name—User name of user.
- Key Type—Whether this is an RSA or DSA key.
- Fingerprint—Fingerprint generated from the public keys.

Step 4 Click **Add or Edit** to add or edit a user and enter the fields:

- SSH User Name—Enter a user name.
- Key Type—Select either RSA or DSA.
- Public Key—Copy the public key generated by an external SSH client application (like PuTTY) into this text box.

Step 5 Click **Apply** to save the new user.

The following fields are displayed for all active users:

- IP Address—IP address of the active user.
- SSH User Name—User name of the active user.

- SSH Version—Version of SSH used by the active user.
- Cipher—Cipher of the active user.
- Authentication Code—Authentication code of the active user.

SSH Server Authentication

A remote SSH client can perform SSH Server Authentication to ensure it's establishing an SSH session to the expected SSH driver. To perform SSH Server Authentication, the remote SSH client must have a copy of the SSH server public key (or fingerprint) of the target SSH server.

The SSH Server Authentication page generates/imports the private/public key for the device as an SSH server. A user should copy the SSH server public key (or fingerprint) of this device to the application if it's to perform an SSH Server Authentication on its SSH sessions. Public and private RSA and DSA keys are automatically generated when the device is booted from the factory defaults. Each key is also automatically created when the appropriate user-configured key is deleted by the user.

To regenerate an RSA or DSA key or to copy in an RSA/DSA key generated on another device, complete the following steps:

Procedure

Step 1 Click **Security** > **SSH Server** > **SSH Server Authentication**.

The following fields are displayed for each key:

- Key Type—RSA or DSA.
- Key Source—Auto Generated or User Defined.
- Fingerprint—Fingerprint generated from the key.

Step 2 Select either an RSA or DSA key.

Step 3 You can perform any of the following actions:

- Generate—Generates a key of the selected type.
- Edit—Enables you to copy in a key from another device. Enter the following fields:
  - Key Type—As described above
  - Public Key—Enter the public key.
  - Private Key—Select either Plaintext or Encrypted and enter the private key.

    Plaintext—Enter the key as plaintext.

Step 4 Click **Apply** to set the settings.

Step 5 Display Sensitive Data as Encrypted- click to display the SSH authentication settings as encrypted.

SSH Client

A SSH client helps the user manage a network composed of one or more switches in which various system files are stored on a central SSH server. When configuration files are transferred over a network, the Secure Copy (SCP), which is an application that utilizes the SSH protocol, ensures that sensitive data, such as username/password cannot be intercepted.

The SSH client, only communicates with a trusted SSH server. When SSH server authentication is disabled (the default setting), any SSH server is considered trusted. When SSH server authentication is enabled, the user must add an entry for the trusted servers to the Trusted SSH Servers Table.

In general the SSH protocol can be used for two purposes, file transfers and terminal access.

SSH User Authentication

When a device (SSH client) attempts to establish a SSH session to a SSH server, the SSH server uses various methods for client authentication. Use this page to select an SSH user authentication method, set a username and password on the device, if the password method is selected or generate an RSA or DSA key, if the public/private key method is selected.

To select an authentication method, and set the username/password/keys, follow these steps:

Procedure

Step 1 Click **Security** > **SSH Client** > **SSH User Authentication**.

Step 2 Select an SSH User Authentication Method. This is the global method defined for the secure copy (SCP). Select one of the options:

- By Password—This is the default setting. If this is selected, enter a password or retain the default one.
- By RSA Public Key—If this is selected, create an RSA public and Private key in the SSH User Key Table block.
- By DSA Public Key—If this is selected, create a DSA public/private key in the SSH User Key Table block.

Step 3 Enter the Username (no matter what method was selected) or user the default username. This must match the username defined on the SSH server.

Step 4 If the By Password method was selected, enter a password (Encrypted or Plaintext) or leave the default encrypted password.

Step 5 Perform one of the following actions:

- Apply—The selected authentication methods are associated with the access method.
- Restore Default Credentials—The default username and password (anonymous) are restored.
- Display Sensitive Data As Plaintext—Sensitive data for the current page appears as plaintext.

The SSH User Key Table contains the following fields for each key:

- Key Type—RSA or DSA.

- Key Source—Auto Generated or User Defined.
- Fingerprint—Fingerprint generated from the key.

Step 6 To handle an RSA or DSA key, select either RSA or DSA and perform one of the following actions:

- Generate—Generate a new key.
- Edit—Display the keys for copying/pasting to another device.
- Delete—Delete the key.
- Details—Display the keys.

SSH Server Authentication

To enable SSH server authentication and define the trusted servers, follow these steps:

Procedure

Step 1 Click **Security** > **SSH Client** > **SSH Server Authentication**.

Step 2 Select **Enable** to enable SSH server authentication.

- IPv4 Source Interface—Select the source interface whose IPv4 address will be used as the source IPv4 address for messages used in communication with IPv4 SSH servers.
- IPv6 Source Interface—Select the source interface whose IPv6 address will be used as the source IPv6 address for messages used in communication with IPv6 SSH servers.

Note
If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

Step 3 Click **Apply**.

Step 4 Click **Add** and enter the following fields for the Trusted SSH Server:

- Server Definition—Select one of the following ways to identify the SSH server:
  - By IP address—If this is selected enter the IP address of the server in the fields below.
  - By name—If this is selected enter the name of the server in the Server IP Address/Name field.
- IP Version—If you selected to specify the SSH server by IP address, select whether that IP address is an IPv4 or IPv6 address.
- IPv6 Address Type—If the SSH server IP address is an IPv6 address, select the IPv6 address type. The options are:
  - Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link

local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.

- Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.

- Link Local Interface—Select the link local interface from the list of interfaces.
- Server IP Address/Name—Enter either the IP address of the SSH server or its name, depending on what was selected in Server Definition.
- Fingerprint—Enter the fingerprint of the SSH server (copied from that server).

Step 5 Click **Apply**. The trusted server definition is stored in the Running Configuration file.

Change User Password on the SSH Server

To change the password on the SSH server, follow these steps:

Procedure

Step 1 Click **Security** > **SSH Client** > **Change User Password on SSH Server**.

Step 2 Enter the following fields:

- Server Definition—Define the SSH server by selecting either By IP Address or By Name. Enter the server name or IP address of the server in the Server IP Address/Name field.
- IP Version—If you selected to specify the SSH server by IP address, select whether that IP address is an IPv4 or IPv6 address.
- IPv6 Address Type—If the SSH server IP address is an IPv6 address, select the IPv6 address type. The options are:
  - Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- Link Local Interface—Select the link local interface from the list of interfaces.
- Server IP Address/Name—Enter either the IP address of the SSH server or its name, depending on what was selected in Server Definition.
- Username—This must match the username on the server.
- Old Password—This must match the password on the server.
- New Password—Enter the new password and confirm it in the Confirm Password field.

Step 3 Click **Apply**. The password on the SSH server is modified.

TCP/UDP Services

The TCP/UDP Services page enables TCP or UDP-based services on the device, usually for security reasons.

The device offers the following TCP/UDP services:

- HTTP-Enabled by factory default
- HTTPS-Enabled by factory default
- SNMP-Disabled by factory default
- Telnet-Disabled by factory default
- SSH-Disabled by factory default

To configure TCP/UDP services, follow these steps:

Procedure

Step 1 Click **Security** > **TCP/UDP Services**.

Step 2 Enable or disable the following TCP/UDP services on the displayed services.

- HTTP Service-Indicates whether the HTTP service is enabled or disabled.
- HTTPS Service-Indicates whether the HTTPS service is enabled or disabled.
- SNMP Service-Indicates whether the SNMP service is enabled or disabled.
- Telnet Service-Indicates whether the Telnet service is enabled or disabled.
- SSH Service-Indicates whether the SSH server service is enabled or disabled.

Step 3 Click **Apply**. The services are written to the Running Configuration file.

The TCP Service Table displays the following fields for each service:

- Service Name-Access method through which the device is offering the TCP service.
- Type-IP protocol the service uses.
- Local IP Address-Local IP address through which the device is offering the service.
- Local Port-Local TCP port through which the device is offering the service.
- Remote IP Address-IP address of the remote device that is requesting the service.
- Remote Port-TCP port of the remote device that is requesting the service.
- State-Status of the service.

The UDP Service table displays the following information:

- Service Name-Access method through which the device is offering the UDP service.
- Type-IP protocol the service uses.

- Local IP Address-Local IP address through which the device is offering the service.
- Local Port-Local UDP port through which the device is offering the service.
- Application Instance-The service instance of the UDP service.

Storm Control

When Broadcast, Multicast, or Unknown Unicast frames are received, they are duplicated, and a copy is sent to all possible egress ports. This means that in practice they are sent to all ports belonging to the relevant VLAN. In this way, one ingress frame is turned into many, creating the potential for a traffic storm.

Storm protection enables you to limit the number of frames entering the device and to define the types of frames that are counted towards this limit.

When the rate of Broadcast, Multicast, or Unknown Unicast frames is higher than the user-defined threshold, frames received beyond the threshold are discarded.

Storm Control Settings

To define Storm Control, follow these steps:

Procedure

Step 1 Click **Security** > **Storm Control** > **Storm Control Settings**.

Step 2 Select a port and click **Edit.**

Step 3 Enter the parameters.

- Interface—Select the port for which storm control is enabled.

  Unknown Unicast Storm Control

- Storm Control State—Select to enable Storm Control for Unicast packets.
- Rate Threshold—Enter the maximum rate at which unknown packets can be forwarded. This value can be entered By kbits/sec or By percentage of the total available bandwidth.
- Trap on Storm—Select to send a trap when a storm occurs on a port. If this isn't selected, the trap isn't sent.
- Shutdown on Storm—Select to shut down a port when a storm occurs on the port. If this isn't selected extra traffic is discarded.

  Multicast Storm Control

- Storm Control State—Select to enable Storm Control for Multicast packets.
- Multicast Type—Select one of the following types of Multicast packets on which to implement storm control:
  - All—Enables storm control on all Multicast packets on the port
  - Registered Multicast—Enables storm control only on registered Multicast addresses on the port

- Unregistered Multicast—Enables only unregistered Multicast storm control on the port

- Rate Threshold—Enter the maximum rate at which unknown packets can be forwarded. This value can be entered By kbits/sec or By percentage of the total available bandwidth.
- Trap on Storm—Select to send a trap when a storm occurs on a port. If this isn't selected, the trap isn't sent.
- Shutdown on Storm—Select to shut down a port when a storm occurs on the port. If this isn't selected extra traffic is discarded.

Broadcast Storm Control

- Storm Control State—Select to enable Storm Control for Broadcast packets.
- Rate Threshold—Enter the maximum rate at which unknown packets can be forwarded. This value can be entered By kbits/sec or By percentage of the total available bandwidth.
- Trap on Storm—Select to send a trap when a storm occurs on a port. If this isn't selected, the trap isn't sent.
- Shutdown on Storm—Select to shut down a port when a storm occurs on the port. If this isn't selected extra traffic is discarded.

Step 4 Click **Apply**. Storm control is modified, and the Running Configuration file is updated.

Storm Control Statistics

To view Storm Control statistics, complete the following:

Procedure

Step 1 Click **Security > Storm Control > Storm Control Statistics**.

Step 2 Select an interface.

Step 3 Enter the Refresh Rate—Select the how often the statistics should be refreshed. The available options are:

No Refresh	Statistics aren't refreshed.
15 Sec	Statistics are refreshed every 15 seconds.
30 Sec	Statistics are refreshed every 30 seconds.
60 Sec	Statistics are refreshed every 60 seconds.

The following statistics are displayed for Unknown Unicast, Multicast and Broadcast Storm Control:

Multicast Traffic Type	(Only for Multicast traffic) All.
Bytes Passed	Number of bytes received.
Bytes Dropped	Number of bytes dropped because of storm control.
Last Drop Time	Time that the last byte was dropped.

Step 4 To clear all counters on all interfaces, click **Clear All Interfaces Counters**. To clear all counters on an interface, select it and click **Clear Interface Counters**.

Port Security



Note Port security cannot be enabled on ports on which 802.1X is enabled or on ports that defined as SPAN destination.

Network security can be increased by limiting access on a port to users with specific MAC addresses. The MAC addresses can be either dynamically learned or statically configured.

Port security monitors received and learned packets. Access to locked ports is limited to users with specific MAC addresses.

Port Security has four modes:

- Classic Lock—All learned MAC addresses on the port are locked, and the port doesn't learn any new MAC addresses. The learned addresses aren't subject to aging or relearning.
- Limited Dynamic Lock—The device learns MAC addresses up to the configured limit of allowed addresses. After the limit is reached, the device doesn't learn additional addresses. In this mode, the addresses are subject to aging and relearning.
- Secure Permanent—Keeps the current dynamic MAC addresses associated with the port (as long as the configuration was saved to the Start configuration file). New MAC addresses can be learned as Permanent Secure ones up to the maximum addresses allowed on the port. Relearning and aging are disabled.
- Secure Delete on Reset—Deletes the current dynamic MAC addresses associated with the port after reset. New MAC addresses can be learned as Delete-On-Reset ones up to the maximum addresses allowed on the port. Relearning and aging are disabled.

When a frame from a new MAC address is detected on a port where it's not authorized (the port is classically locked, and there's a new MAC address, or the port is dynamically locked, and the maximum number of allowed addresses has been exceeded), the protection mechanism is invoked, and one of the following actions can take place:

- Frame is discarded.
- Frame is forwarded.
- Port is shut down.

When the secure MAC address is seen on another port, the frame is forwarded, but the MAC address isn't learned on that port.

In addition to one of these actions, you can also generate traps, and limit their frequency and number to avoid overloading the devices.

To configure port security, complete the following:

Procedure

Step 1 Click **Security** > **Port Security**.

Step 2 Select an interface to be modified, and click **Edit.**

Step 3 Enter the parameters.

- Interface—Select the interface name.
- Interface Status—Select to lock the port.
- Learning Mode—Select the type of port locking. To configure this field, the Interface Status must be unlocked. The Learning Mode field is enabled only if the Interface Status field is locked. To change the Learning Mode, the Lock Interface must be cleared. After the mode is changed, the Lock Interface can be reinstated. The options are:
  - Classic Lock—Locks the port immediately, regardless of the number of addresses that have already been learned.
  - Limited Dynamic Lock—Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both relearning and aging of MAC addresses are enabled.
  - Secure Permanent—Keeps the current dynamic MAC addresses associated with the port and learns up to the maximum number of addresses allowed on the port (set by Max No. of Addresses Allowed). Relearning and aging are disabled.
  - Secure Delete on Reset—Deletes the current dynamic MAC addresses associated with the port after reset. New MAC addresses can be learned as Delete-On-Reset ones up to the maximum addresses allowed on the port. Relearning and aging are disabled.
- Max No. of Addresses Allowed—Enter the maximum number of MAC addresses that can be learned on the port if Limited Dynamic Lock learning mode is selected. The number 0 indicates that only static addresses are supported on the interface.
- Action on Violation—Select an action to be applied to packets arriving on a locked port. The options are:
  - Discard—Discards packets from any unlearned source
  - Forward—Forwards packets from an unknown source without learning the MAC address
  - Shutdown—Discards packets from any unlearned source, and shuts down the port The port remains shut down until reactivated, or until the device is rebooted.
- Trap—Select to enable traps when a packet is received on a locked port. This is relevant for lock violations. For Classic Lock, this is any new address received. For Limited Dynamic Lock, this is any new address that exceeds the number of allowed addresses.
- Trap Frequency—Enter minimum time (in seconds) that elapses between traps.

Step 4 Click **Apply**. Port security is modified, and the Running Configuration file is updated.

802.1X Authentication

802.1x authentication restricts unauthorized clients from connecting to a LAN through publicity-accessible ports. 802.1x authentication is a client-server model. In this model, network devices have the following specific roles.

- Client or supplicant
- Authenticator
- Authentication server

A network device can be either a client/supplicant, authenticator or both per port.

802.1X Authentication Properties

The Properties page is used to globally enable port/device authentication. For authentication to function, it must be activated both globally and individually on each port.

To define port-based authentication, follow these steps:

Procedure

Step 1 Click **Security > 802.1X Authentication > Properties**.

Step 2 Enter the parameters.

- Port-Based Authentication—Enable or disable port-based authentication.
- Authentication Method—Select the user authentication methods. The options are:
  - RADIUS, None—Perform port authentication first by using the RADIUS server. If no response is received from RADIUS, then no authentication is performed, and the session is permitted.
  - RADIUS—Authenticate the user on the RADIUS server. If no authentication is performed, the session isn't permitted.
  - None—Don't authenticate the user. Permit the session.
- Guest VLAN—Select to enable the use of a guest VLAN for unauthorized ports. If a guest VLAN is enabled, all unauthorized ports automatically join the VLAN selected in the Guest VLAN ID field. If a port is later authorized, it's removed from the guest VLAN.

  The guest VLAN can be defined as a layer 3 interface (assigned an IP address) like any other VLAN. However, device management isn't available via the guest VLAN IP address.
- Guest VLAN ID—Select the guest VLAN from the list of VLANs.
- Guest VLAN Timeout—Define a time period as either Immediate or enter a value in User Defined. This value is used as follows:

  After linkup, if the software doesn't detect the 802.1X supplicant, or the authentication has failed, the port is added to the guest VLAN, only after the Guest VLAN timeout period has expired.

If the port state changes from Authorized to Not Authorized, the port is added to the guest VLAN only after the Guest VLAN timeout has expired.

- Trap Settings—To enable traps, select one of more of the following options:
  - 802.1x Authentication Failure Traps—Select to generate a trap if 802.1x authentication fails.
  - 802.1x Authentication Success Traps—Select to generate a trap if 802.1x authentication succeeds.
  - MAC Authentication Failure Traps—Select to generate a trap if MAC authentication fails.
  - MAC Authentication Success Traps—Select to generate a trap if MAC authentication succeeds.
  - Supplicant Authentication Failure Traps—Select to generate a trap if supplicant authentication fails.
  - Supplicant Authentication Success Traps—Select to generate a trap if supplicant authentication succeeds.
  - Web Authentication Failure Traps—Select to generate a trap if Web authentication fails.
  - Web Authentication Success Traps—Select to generate a trap if Web authentication succeeds.
  - Web Authentication Quiet Traps—Select to generate a trap if a quiet period commences.

  The VLAN Authentication Table displays all VLANs, and indicates whether authentication has been enabled on them.

Step 3 Click **Apply**. The 802.1X properties are written to the Running Configuration file.

To change Enable or Disable authentication on a VLAN, click **Edit** and select VLAN and either Enable or Disable.

Port Authentication

The Port Authentication page enables configuration of parameters for each port. Since some of the configuration changes are only possible while the port is in Force Authorized state, such as host authentication, it's recommended that you change the port control to Force Authorized before making changes. When the configuration is complete, return the port control to its previous state.

Note A port with 802.1x defined on it can't become a member of a LAG. 802.1x and Port Security can't be enabled on same port at same time. If you enable port security on an interface, the Administrative Port Control can't be changed to Auto mode.

To define 802.1X authentication:

Procedure

Step 1 Click **Security** > **802.1X Authentication** > **Port Authentication**.

This page displays authentication settings for all ports.

In addition to the fields described on the Add page, the following fields are displayed for each port:

- Supplicant Status—Either Authorized or Unauthorized for an interface on which 802.1x supplicant has been enabled.
- Supplicant Credentials—Name of the credential structure used for the supplicant interface, so the possible value is any name or N/A if the supplicant isn't enabled. If a port has a configured supplicant credential name, the value for the port control parameters is Supplicant. This value overrides any other port control information received from the port.

Step 2 Select a port and click **Edit.**

Step 3 Enter the parameters.

- Interface—Select a port.
- Current Port Control—Displays the current port authorization state. If the state is Authorized, the port is either authenticated or the Administrative Port Control is Force Authorized. Conversely, if the state is Unauthorized, then the port is either not authenticated or the Administrative Port Control is Force Unauthorized. If supplicant is enabled on an interface, the current port control is Supplicant.
- Administrative Port Control—Select the Administrative Port Authorization state. The options are:
  - Force Unauthorized—Denies the interface access by moving the interface into the unauthorized state. The device doesn't provide authentication services to the client through the interface.
  - Auto—Enables port-based authentication and authorization on the device. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.
  - Force Authorized—Authorizes the interface without authentication.
- RADIUS VLAN Assignment—Select to enable Dynamic VLAN assignment on the selected port.
  - Disable—Feature is not enabled.
  - Reject—If the RADIUS server authorized the supplicant, but didn't provide a supplicant VLAN, the supplicant is rejected.
  - Static—If the RADIUS server authorized the supplicant, but didn't provide a supplicant VLAN, the supplicant is accepted.
- Guest VLAN—Select to enable using a guest VLAN for unauthorized ports.
- Open Access—Select to successfully authenticate the port even though authentication fails.
- 802.1X Based Authentication—Select to enable 802.1X authentication on the port.
- MAC-Based Authentication—Select to enable port authentication based on the supplicant MAC address. Only 8 MAC-based authentications can be used on the port.

  Note
  For MAC authentication to succeed, the RADIUS server supplicant username and password must be the supplicant MAC address. The MAC address must be in lower case letters and entered without the. Or - separators; for example: 0020aa00bbcc.

- Web-Based Authentication—Select to enable web-based authentication based on the supplicant MAC address.
- Periodic Reauthentication—Select to enable port reauthentication attempts after the specified Reauthentication Period.
- Reauthentication Period—Enter the number of seconds after which the selected port is reauthenticated.

- Reauthenticate Now—Select to enable immediate port reauthentication.
- Authenticator State—Displays the defined port authorization state. The options are:
  - Initialize—In process of coming up.
  - Force-Authorized—Controlled port state is set to Force-Authorized (forward traffic).
  - Force-Unauthorized—Controlled port state is set to Force-Unauthorized (discard traffic).

  Note
  If the port isn't in Force-Authorized or Force-Unauthorized, it's in Auto Mode and the authenticator displays the state of the authentication in progress. After the port is authenticated, the state is shown as Authenticated.

- Time Range—Select to enable limiting authentication to a specific time range.
- Time Range Name—If Time Range is selected, click the Edit button to be redirected to the time range page and select the time range name to be used.
- Maximum WBA Login Attempts—Enter the maximum number of login attempts allowed for web-based authentication. Select either Infinite for no limit or User Defined to set a limit.
- Maximum WBA Silence Period—Enter the maximum length of the silent period for web-based authentication allowed on the interface. Select either Infinite for no limit or User Defined to set a limit.
- Max Hosts—Enter the maximum number of authorized hosts allowed on the interface.

  Select either Infinite for no limit, or User Defined to set a limit.

  Note
  Set this value to 1 to simulate single-host mode for web-based authentication in multi-sessions mode.

- Quiet Period—Enter the length of the quiet period.
- Resending EAP—Enter the number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request.
- Max EAP Requests—Enter the maximum number of EAP requests that will be sent. If a response isn't received after the defined period (supplicant timeout), the authentication process is restarted.
- EAP Max Retries—Enter the maximum number of EAP retries that can be sent.
- EAP Timeout—Enter the maximum time that is waited for EAP responses before timeout occurs.
- Supplicant Timeout—Enter the number of seconds that lapses before EAP requests are resent to the supplicant.
- Server Timeout—Enter the number of seconds that lapses before the device resends a request to the authentication server.
- Supplicant—Select to enable 802.1X.
- Credentials—Select credentials from the drop-down list to use for this supplicant. This parameter is available only if supplicant is enabled on the interface. Edit links to the Supplicant Credentials page where credentials can be configured.
- Supplicant Held Timeout—Enter the time period during which the supplicant waits before restarting authentication after receiving the FAIL response from the RADIUS server.

Step 4 Click **Apply**. The port settings are written to the Running Configuration file.

Host and Session Authentication

The Host and Session Authentication page enables defining the mode in which 802.1X operates on the port and the action to perform if a violation has been detected.

To define 802.1X advanced settings for ports, complete the following steps:

Procedure

Step 1 Click **Security** > **802.1X Authentication** > **Host and Session Authentication**.

The authentication parameters are described for all ports. All fields except the following are described in the Edit page.

- Number of Violations—Displays the number of packets that arrive on the interface in single-host mode, from a host whose MAC address isn't the supplicant MAC address.

Step 2 Select a port, and click **Edit.**

Step 3 Enter the parameters.

- Interface—Enter a port number for which host authentication is enabled.
- Host Authentication—Select from one of the following modes.
  - Single Host—A port is authorized if there is an authorized client. Only one host can be authorized on a port.
  - Multiple Host (802.1x)—A port is authorized if there is if there is at least one authorized client.
  - Multiple Sessions—Unlike the single-host and multi-host modes, a port in the multi-session mode does not have an authentication status. This status is assigned to each client connected to the port.

  Single Host Violation Settings—Can only be chosen if host authentication is Single Host.
- Action on Violation—Select the action to be applied to packets arriving in Single Session/Single Host mode, from a host whose MAC address isn't the supplicant MAC address. The options are:
  - Protect (Discard)—Discards the packets.
  - Restrict (Forward)—Forwards the packets.
  - Shutdown—Discards the packets and shuts down the port. The ports remain shut down until reactivated, or until the device is rebooted.
- Traps—Select to enable traps.
- Trap Frequency—Defines how often traps are sent to the host. This field can be defined only if multiple hosts are disabled.

Step 4 Click **Apply**. The settings are written to the Running Configuration file.

Supplicant Credentials

In addition to its capacity as an 802.1x authenticator, the switch itself can be configured as an 802.1x supplicant seeking port access permission from a neighbor. The supplicant supports the EAP MD5-Challenge method specified by RFC3748. The method authenticates a client by its name and password. When the supplicant is enabled on an interface, the interface becomes unauthorized. When the 802.1X authentication process succeeds, the interface state is changed to authorized. This page enables creating and configuring credentials that can be used by an interface configured as an 802.1x supplicant.

To add a supplicant's credentials, complete the following steps:

Procedure

Step 1 Click **Security** > **802.1X Authentication** > **Supplicant Credentials**.

Step 2 Click **Add**.

Step 3 Enter the following fields:

- Credential Name—Name by which to identify the credential.
- User Name—Enter the user name associated with the credential name.
- Description—Enter text describing the user.
- Password—Select the type of password: Encrypted or Plaintext and add the password.

Step 4 Click **Apply** and the settings are saved to the Running Configuration file.

MAC-Based Authentication Settings

MAC-based authentication is an alternative to 802.1X authentication that allows network access to devices (such as printers and IP phones) that do not have the 802.1X supplicant capability. MAC-based authentication uses the MAC address of the connecting device to grant or deny network access.

To configure MAC-based authentication, complete the following steps:

Procedure

Step 1 Click **Security 802.1X Authentication** > **MAC-Based Authentication Settings**

Step 2 Enter the following fields:

- MAC Authentication Type—Select one of the following options:
  - EAP—Use RADIUS with EAP encapsulation for the traffic between the switch (RADIUS client) and the RADIUS server, which authenticates a MAC-based supplicant.
  - RADIUS—Use RADIUS without EAP encapsulation for the traffic between the switch (RADIUS client) and the RADIUS server, which authenticates a MAC-based supplicant.

Username Format

In MAC-based authentication, the supplicant's username is based on the supplicant device MAC address. The following defines the format of this MAC-based username, which is sent from the switch to the RADIUS server, as part of the authentication process.

- Group Size—Number of ASCII characters between delimiters of the MAC address sent as a user name.
- Group Separator—Character used as a delimiter between the defined groups of characters in the MAC address.
- Case—Send user name in lower or upper case.

MAC Authentication Password

- Password—Defines the password that the switch uses for authentication via the RADIUS server. Select one of the following options:
  - Use default (Username)—Select this to use the defined username as the password.
  - Encrypted—Define a password in encrypted format.
  - Plaintext—Define a password in plaintext format.
- Password MD5 Digest—Displays the MD5 Digest password.

Step 3 Click **Apply** and the settings are saved to the Running Configuration file. Click **Display Sensitive Data as Plaintext** to display the password if it is encrypted.

Authenticated Hosts

To view details about authenticated users, click. **Security** > **802.1X Authentication** > **Authenticated Hosts**.

This page displays the following fields:

- User Name—Supplicant names that authenticated on each port.
- Port—Number of the port
- Session Time (DD:HH:MM:SS)—Amount of time that the supplicant was authenticated and authorized access at the port.
- Authentication Method—Method by which the last session was authenticated.
- Authentication Server—RADIUS server
- MAC Address—Displays the supplicant MAC address.
- VLAN ID—Port’s VLAN

Locked Clients

To view clients who have been locked out because of failed login attempts and to unlock a locked client, follow these steps:

Procedure

Step 1 Click **Security** > **802.1X Authentication** > **Locked Client**.

The following fields are displayed:

- Interface—Port that is locked.
- MAC Address—Displays the MAC address of locked station
- Remaining Time (Sec)—The time remaining for the port to be locked.

Step 2 Select a port.

Step 3 Click **Unlock**.

Web Authentication Customization

This page enables designing web-based authentication pages in various languages.

You can add up to 4 languages.



Note Up to 5 HTTP users and one HTTPS user can request web-based authentication at the same time. When these users are authenticated, more users can request authentication.

To add a language for web-based authentication, complete the following:

Procedure

Step 1 Click **Security** > **802.1X Authentication** > **Web Authentication Customization**.

Step 2 Click **Add**.

Step 3 Select a language from the Language drop-down list.

Step 4 Select **Set as Default Display Language** if this language is the default language. the default language pages are displayed if the end user does not select a language.

Step 5 Click **Apply** and the settings are saved to the Running Configuration file.

To customize the web-authentication pages:

Step 6 Click **Security** > **802.1X Authentication** > **Web Authentication Customization.**

This page displays the languages that can be customized.

Step 7 Click **Edit Login Page**.

Step 8 Click **Edit labeled 1**. The following fields are displayed:

- Language—Displays the page's language.

- Color Scheme—Select one of the contrast options.

  If the Custom color scheme is selected, the following options are available:

  - Page Background Color—Enter the ASCII code of the background color. The selected color is shown in the Text field.
  - Page Text Color—Enter the ASCII code of the text color. The selected color is shown in the Text field.
  - Header and Footer Background Color—Enter the ASCII code of the header and footer background color. The selected color is shown in the Text field.
  - Header and Footer Text Color—Enter the ASCII code of the header and footer text color. The selected color is shown in the Text field.
  - Hyperlink Color—Enter the ASCII code of the hyperlink color. The selected color is shown in the Text field.

- Current Logo Image—Displays the name of the file containing the current logo image.
- Logo Image—Select one of the following options:
  - None—No logo
  - Default—Use the default logo.
  - Other—Select to enter a customized logo.

    If the Other logo option is selected, the following options are available:

  - Logo Image Filename—Enter the logo file name or Browse to the image.
  - Application Text—Enter text to accompany the logo.
  - Window Title Text—Enter a title for the Login page.

Step 9 Click **Apply** and the settings are saved to the Running Configuration file.

Step 10 Click **Edit labeled 2**. The following fields are displayed:

- Invalid User Credentials—Enter the text of the message to be displayed when the end user enters an invalid username or password.
- Service Not Available—Enter the text of the message to be displayed when the authentication service isn't available.

Step 11 Click **Apply** and the settings are saved to the Running Configuration file.

Step 12 Click **Edit labeled 3**. The following fields are displayed:

- Welcome Message—Enter the text of the message to be displayed when the end user logs on.
- Instructional Message—Enter the instructions to be displayed to the end user.
- RADIUS Authentication—Displays whether RADIUS authentication is enabled. If so, the username and password must be included in the login page.
- Username Textbox—Select for a username textbox to be displayed.
- Username Textbox Label—Select the label to be displayed before the username textbox.
- Password Textbox—Select for a password textbox to be displayed.

- Password Textbox Label—Select the label to be displayed before the password textbox.
- Language Selection—Select to enable the end user to select a language.
- Language Dropdown Label—Enter the label of the language selection dropdown.
- Login Button Label—Enter the label of the login button.
- Login Progress Label—Enter the text that will be displayed during the login process.

Step 13 Click **Apply** and the settings are saved to the Running Configuration file.

Step 14 Click **Edit labeled 4**. The following fields are displayed:

- Terms and Conditions—Select to enable a terms and conditions text box.
- Terms and Conditions Warning—Enter the text of the message to be displayed as instructions to enter the terms and conditions.
- Terms and Conditions Content—Enter the text of the message to be displayed as terms and conditions.

Step 15 Click **Apply** and the settings are saved to the Running Configuration file.

Step 16 In **Edit labeled 5**, the following fields are displayed:

- Copyright—Select to enable displaying copyright text.
- Copyright Text—Enter the copyright text.

Step 17 Click **Apply** and the settings are saved to the Running Configuration file.

Step 18 Click **Edit Success Page**.

Step 19 Click **Edit** on the right side of the page.

Step 20 Enter the Success Message, which is the text that will be displayed if the end user successfully logs in.

Step 21 Click **Apply** and the settings are saved to the Running Configuration file.

To preview the login or success message, click **Preview**.

To set the default language of the GUI interface as the default language for Web-based authentication, click **Set Default Display Language**.

Denial of Service Prevention

A Denial of Service (DoS) attack is a hacker attempt to make a device unavailable to its users.

DoS attacks saturate the device with external communication requests, so that it cannot respond to legitimate traffic. These attacks usually lead to a device CPU overload.

One method of resisting DoS attacks employed by the device is the use of Secure Core Technology (SCT), which is enabled by default and cannot be disabled. The Cisco device is an advanced device that handles management traffic, protocol traffic and snooping traffic, in addition to end-user (TCP) traffic. SCT ensures that the device receives and processes management and protocol traffic, no matter how much total traffic is received. This is done by rate-limiting TCP traffic to the CPU.

Security Suite Settings

Note Before activating DoS Prevention, you must unbind all Access Control Lists (ACLs) or advanced QoS policies that are bound to a port. ACL and advanced QoS policies aren't active when a port has DoS Protection enabled on it.

To configure DoS Prevention global settings and monitor SCT:

Procedure

Step 1 Click **Security** > **Denial of Service Prevention** > **Security Suite Settings**.

CPU Protection Mechanism: Enabled indicates that SCT is enabled.

Step 2 Click **Details** beside CPU Utilization to go to the CPU Utilization, on page 35 page and view CPU resource utilization information.

Step 3 Click **Edit** beside TCP SYN Protection to set the feature.

Step 4 Configure the DoS Prevention settings:

- Disable-Disable all types of Denial of Service features (except device level TCP SYN protection).
- System-Level Prevention-Enable preventing attacks from Stacheldraht Distribution, Invasor Trojan, Back Orifice Trojan and Martian Addresses.
- System-Level and Interface-Level Prevention-In addition to the system-level prevention, you can enable and configure the following interface-level settings: Syn Filtering, Syn Rate Protection, ICMP Filtering and IP Fragmented.

Step 5 If System-Level Prevention or System-Level and Interface-Level Prevention is selected, enable one or more of the following Denial of Service Protection options:

- Stacheldraht Distribution-Discards TCP packets with source TCP port equal to 16660.
- Invasor Trojan-Discards TCP packets with destination TCP port equal to 2140 and source TCP port equal to 1024.
- Back Orifice Trojan-Discards UDP packets with destination UDP port equal to 31337 and source UDP port equal to 1024.

Step 6 Click the following as required:

- Martian Addresses-Click **Edit** to go to the Martian Addresses, on page 301 page.
- SYN Filtering-Click **Edit** to go to the SYN Filtering, on page 302 page.
- SYN Rate Protection-(In Layer 2 only) Click **Edit** to go to the SYN Rate Protection, on page 302 page.
- ICMP Filtering-Click **Edit** to go to the ICMP Filtering, on page 303 page.
- IP Fragmented-Click **Edit** to go to the IP Fragments Filtering, on page 304 page.

Step 7 Click **Apply**. The Denial of Service prevention Security Suite settings are written to the Running Configuration file.

SYN Protection

The network ports might be used by hackers to attack the device in a SYN attack, which consumes TCP resources (buffers) and CPU power.

Since the CPU is protected using SCT, TCP traffic to the CPU is limited. However, if one or more ports are attacked with a high rate of SYN packets, the CPU receives only the attacker packets, thus creating Denial-of-Service.

When using the SYN protection feature, the CPU counts the SYN packets ingressing from each network port to the CPU per second.

To configure SYN protection, follow these steps:

Procedure

Step 1 Click **Security** > **Denial of Service Prevention** > **SYN Protection**.

Step 2 Enter the parameters.

- Block SYN-FIN Packets-Select to enable the feature. All TCP packets with both SYN and FIN flags are dropped on all ports.
- SYN Protection Mode-Select between three modes:
  - Disable-The feature is disabled on a specific interface.
  - Report-Generates a SYSLOG message. The status of the port is changed to Attacked when the threshold is passed
  - Block and Report-When a TCP SYN attack is identified, TCP SYN packets destined for the system are dropped and the status of the port is changed to Blocked.
- SYN Protection Threshold-Number of SYN packets per second before SYN packets will be blocked (deny SYN with MAC-to-me rule will be applied on the port).
- SYN Protection Period-Time in seconds before unblocking the SYN packets (the deny SYN with MAC-to-me rule is unbound from the port).

Step 3 Click **Apply**. SYN protection is defined, and the Running Configuration file is updated.

The SYN Protection Interface Table displays the following fields for every port or LAG (as requested by the user).

- Current Status-Interface status. The possible values are:
  - Normal-No attack was identified on this interface.
  - Blocked-Traffic isn’t forwarded on this interface.
  - Attacked-Attack was identified on this interface.

- Last Attack-Date of last SYN-FIN attack identified by the system and the system action.

Martian Addresses

The Martian Addresses page enables entering IP addresses that indicate an attack if they are seen on the network. Packets from these addresses are discarded. The device supports a set of reserved Martian addresses that are illegal from the point of view of the IP protocol. The supported reserved Martian addresses are:

- Addresses defined to be illegal in the Martian Addresses page
- Addresses that are illegal from the point of view of the protocol, such as loopback addresses, including addresses within the following ranges:
  - 0.0.0.0/8 (Except 0.0.0.0/32 as a Source Address)-Addresses in this block refer to source hosts on this network.
  - 127.0.0.0/8-Used as the Internet host loopback address
  - 192.0.2.0/24-Used as the TEST-NET in documentation and example codes
  - 224.0.0.0/4 (As a Source IP Address)-Used in IPv4 Multicast address assignments, and was formerly known as Class D Address Space.
  - 240.0.0.0/4 (Except 255.255.255.255/32 as a Destination Address)-Reserved address range, and was formerly known as Class E Address Space.

You can also add new Martian Addresses for DoS prevention. Packets that have a Martian address are discarded.

To define Martian addresses, follow these steps:

Procedure

Step 1 Click **Security** > **Denial of Service Prevention** > **Martian Addresses**.

Step 2 Select **Reserved Martian Addresses** and click **Apply** to include the reserved Martian Addresses in the System Level Prevention list.

Step 3 To add a Martian address click **Add**.

Step 4 Enter the parameters.

- IP Version-Indicates the supported IP version. Currently, support is only offered for IPv4.
- IP Address-Enter an IP address to reject. The possible values are:
  - From Reserved List-Select a well-known IP address from the reserved list.
  - New IP Address-Enter an IP address.
- Mask-Enter the mask of the IP address to define a range of IP addresses to reject. The values are:
  - Network Mask-Network mask in dotted decimal format

- Prefix Length-Enter the prefix of the IP address to define the range of IP addresses for which Denial of Service prevention is enabled.

Step 5 Click **Apply**.

SYN Filtering

The SYN Filtering page enables filtering TCP packets that contain a SYN flag, and are destined for one or more ports.

To define a SYN filter, complete the following steps:

Procedure

Step 1 Click **Security** > **Denial of Service Prevention** > **SYN Filtering**.

Step 2 Click **Add**.

Step 3 Enter the parameters.

- Interface—Select the interface on which the filter is defined.
- IPv4 Address—Enter the IP address for which the filter is defined, or select All addresses.
- Network Mask—Enter the network mask for which the filter is enabled in IP address format. Enter one of the following:
  - Mask—Network mask in dotted decimal format
  - Prefix length—Enter the Prefix length of the IP address to define the range of IP addresses for which Denial of Service prevention is enabled.
- TCP Port—Select the destination TCP port being filtered:
  - Known ports—Select a port from the list.
  - User Defined—Enter a port number.
  - All ports—Select to indicate that all ports are filtered.

Step 4 Click **Apply**. The SYN filter is defined, and the Running Configuration file is updated.

SYN Rate Protection

The SYN Rate Protection page enables limiting the number of SYN packets received on the ingress port. This can mitigate the effect of a SYN flood against servers, by rate limiting the number of new connections opened to handle packets.

To define SYN rate protection, complete the following steps:

Procedure

Step 1 Click **Security** > **Denial of Service Prevention** > **SYN Rate Protection**.

Step 2 Click **Add**.

Step 3 Enter the parameters.

- Interface—Select the interface on which the rate protection is being defined.
- IP Address—Enter the IP address for which the SYN rate protection is defined or select All addresses. If you enter the IP address, enter either the mask or prefix length.
- Network Mask—Select the format for the subnet mask for the source IP address, and enter a value in one of the fields:
  - Mask—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
  - Prefix length—Select the Prefix length and enter the number of bits that comprise the source IP address prefix.
- SYN Rate Limit—Enter the number of SYN packets that be received.

Step 4 Click **Apply**. The SYN rate protection is defined, and the Running Configuration is updated.

ICMP Filtering

The ICMP Filtering page enables the blocking of ICMP packets from certain sources. This can reduce the load on the network in case of an ICMP attack.

To configure the ICMP filtering, complete the following steps:

Procedure

Step 1 Click **Security** > **Denial of Service Prevention** > **ICMP Filtering**.

Step 2 Click **Add**.

Step 3 Enter the parameters.

- Interface—Select the interface on which the ICMP filtering is being defined.
- IP Address—Enter the IPv4 address for which the ICMP packet filtering is activated or select All addresses to block ICMP packets from all source addresses. If you enter the IP address, enter either the mask or prefix length.
- Network Mask—Select the format for the subnet mask for the source IP address, and enter a value in one of the field:
  - Mask—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
  - Prefix length—Select the Prefix length and enter the number of bits that comprise the source IP address prefix.

Step 4 Click **Apply**. The ICMP filtering is defined, and the Running Configuration is updated.

IP Fragments Filtering

IP fragmentation occurs when the data of the network layer is too large to be transmitted over the data link layer in one piece. Then the data of the network layer is split into several pieces (fragments), and this process is called IP fragmentation.

To configure fragmented IP filtering and block fragmented IP packets, complete the following steps:

Procedure

Step 1 Click **Security** > **Denial of Service Prevention** > **IP Fragments Filtering**.

Step 2 Click **Add**.

Step 3 Enter the parameters.

- Interface—Select the interface on which the IP fragmentation is being defined.
- IP Address—Enter an IP network from which the fragmented IP packets is filtered or select All addresses to block IP fragmented packets from all addresses. If you enter the IP address, enter either the mask or prefix length.
- Network Mask—Select the format for the subnet mask for the source IP address, and enter a value in one of the fields:
  - Mask—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
  - Prefix length—Select the Prefix length and enter the number of bits that comprise the source IP address prefix.

Step 4 Click **Apply**. The IP fragmentation is defined, and the Running Configuration file is updated.

IP Source Guard

IP Source Guard is a security feature that can be used to prevent traffic attacks caused when a host tries to use the IP address of its neighbor.

When IP Source Guard is enabled, the device only transmits client IP traffic to IP addresses contained in the DHCP Snooping Binding database. This includes both addresses added by DHCP Snooping and manually-added entries. If the packet matches an entry in the database, the device forwards it. If not, it is dropped.

If IP Source Guard is enabled on a port then:

- DHCP packets allowed by DHCP Snooping are permitted
- If source IP address filtering is enabled:
  - IPv4 traffic: Only traffic with a source IP address that is associated with the port is permitted.

- Non IPv4 traffic: Permitted (Including ARP packets).

IP Source Guard Properties

To enable IP Source Guard globally:

Procedure

Step 1 Click **Security > IP Source Guard > Properties**.

Step 2 Select **Enable** to enable IP Source Guard globally.

Step 3 Click **Apply** to enable IP Source Guard.

Interface Settings

If IP Source Guard is enabled on an untrusted port/LAG, DHCP packets, allowed by DHCP Snooping, are transmitted. If source IP address filtering is enabled, packet transmission is permitted as follows:

- IPv4 traffic—Only IPv4 traffic with a source IP address that is associated with the specific port is permitted.
- Non IPv4 traffic—All non-IPv4 traffic is permitted.

To configure IP Source Guard on interfaces:

Procedure

Step 1 Click **Security** > **IP Source Guard** > **Interface Settings.**

Step 2 Select port/LAG from the Filter field and click **Go**. The ports/LAGs on this unit are displayed along with the following:

- IP Source Guard—Indicates whether IP Source Guard is enabled on the port.
- DHCP Snooping Trusted Interface—Indicates whether this is a DHCP trusted interface.

Step 3 Select the port/LAG and click **Edit**. Select **Enable** in the IP Source Guard field to enable IP Source Guard on the interface.

Step 4 Click **Apply** to copy the setting to the Running Configuration file.

IP Source Guard Binding Database

IP Source Guard uses the DHCP Snooping - to check packets from untrusted ports. If the device attempts to write too many entries to the DHCP Snooping -, the excessive entries are maintained in an inactive status. Entries are deleted when their lease time expires and so inactive entries may be made active.

See DHCP Snooping/Relay, on page 214.

Note The page only displays the entries in the DHCP Snooping - defined on IP-Source-Guard-enabled ports.

To view the DHCP Snooping - and see TCAM resources consumed, complete the following:

Procedure

Step 1 Click **Security** > **IP Source Guard** > **Binding Database.**

The Supported IP Format and TCAM Resources Consumed will be displayed.

Step 2 The DHCP Snooping uses TCAM resources for managing the database. Complete the Insert Inactive field to select how frequently the device should attempt to activate inactive entries. It has the following options:

- Retry Frequency—The frequency with which the TCAM resources are checked.
- Never-Never try to reactivate inactive addresses.

Step 3 Click **Apply** to save the above changes to the Running Configuration and/or Retry Now to check TCAM resources.

The following entries are displayed:

- VLAN ID—VLAN on which packet is expected.
- MAC Address—MAC address to be matched.
- IP Address—IP address to be matched.
- Interface—Interface on which packet is expected.
- Status—Displays whether interface is active.
- Type—Displays whether entry is dynamic or static.
- Reason—If the interface isn't active, displays the reason. The following reasons are possible:
  - No Problem—Interface is active.
  - No Snoop VLAN—DHCP Snooping isn't enabled on the VLAN.
  - Trusted Port—Port has become trusted.
  - Resource Problem—TCAM resources are exhausted.

Step 4 To see a subset of these entries, enter the relevant search criteria and click **Go**.

ARP Inspection

ARP enables IP communication within a Layer 2 Broadcast domain by mapping IP addresses to a MAC addresses.

A malicious user can attack hosts, switches, and routers connected to a 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. This can happen because ARP allows a gratuitous reply from a host even if an ARP request was not received. After the attack, all traffic from the device under attack flows through the attacker's computer and then to the router, switch, or host.

Hosts A, B, and C are connected to the switch on interfaces A, B and C, all of which are on the same subnet. Their IP, MAC addresses are shown in parentheses; for example, Host A uses IP address IA and MAC address MA. When Host A needs to communicate with Host B at the IP layer, it broadcasts an ARP request for the MAC address associated with IP address IB. Host B responds with an ARP reply. The switch and Host A update their ARP cache with the MAC and IP of Host B.

Host C can poison the ARP caches of the switch, Host A, and Host B by broadcasting forged ARP responses with bindings for a host with an IP address of IA (or IB) and a MAC address of MC. Hosts with poisoned ARP caches use the MAC address MC as the destination MAC address for traffic intended for IA or IB, which enables Host C intercepts that traffic. Because Host C knows the true MAC addresses associated with IA and IB, it can forward the intercepted traffic to those hosts by using the correct MAC address as the destination. Host C has inserted itself into the traffic stream from Host A to Host B, the classic man-in-the-middle attack.

ARP Inspection Properties

To configure ARP Inspection properties:

Procedure

Step 1 Click **Security** > **ARP Inspection** > **Properties**.

Enter the following fields:

- ARP Inspection Status-Select to enable ARP Inspection.
- ARP Packet Validation-Select to enable validation checks.
- Log Buffer Interval-Select one of the following options:
  - Retry Frequency-Enable sending SYSLOG messages for dropped packets. Entered the frequency with which the messages are sent.
  - Never-Disabled SYSLOG dropped packet messages.

Step 2 Click **Apply**. The settings are defined, and the Running Configuration file is updated.

ARP Inspection Interfaces Settings

Packets from untrusted ports/LAGs are checked against the ARP Access Rules table and the DHCP Snooping Binding database if DHCP Snooping is enabled (see the DHCP Snooping Binding Database, on page 219).

By default, ports/LAGs are ARP Inspection untrusted.

To change the ARP trusted status of a port/LAG:

Procedure

Step 1 Click **Security** > **ARP Inspection** > **Interface Settings**.

The ports/LAGs and their ARP trusted/untrusted status are displayed.

Step 2 To set a port/LAG as trusted or untrusted, select the port/LAG and click **Edit**.

Step 3 Select **Trusted** or **Untrusted** and click **Apply** to save the settings to the Running Configuration file.

ARP Access Control

To add entries to the ARP Inspection table:

Procedure

Step 1 Click **Security** > **ARP Inspection** > **ARP Access Control**.

Step 2 To add an entry, click **Add**.

Step 3 Enter the fields:

- ARP Access Control Name-Enter a user-created name.
- IP Address-IP address of packet.
- MAC Address-MAC address of packet.

Step 4 Click **Apply**. The settings are defined, and the Running Configuration file is updated.

ARP Access Control Rules

To add more rules to a previously-created ARP Access Control group:

Procedure

Step 1 Click **Security** > **ARP Inspection** > **ARP Access Control Rules**.

The ARP Access Control Rule Table displays, with the currently-defined access rules.

To select a specific group, select Filter, select the control name and click **Go**.

Step 2 To add more rules to a group, click **Add**.

Step 3 Select an ARP Access Control Name and enter the fields:

- IP Address-IP address of packet.

- MAC Address-MAC address of packet.

Step 4 Click **Apply**. The settings are defined, and the Running Configuration file is updated.

ARP Inspection VLAN Settings

To enable ARP Inspection on VLANs and associate Access Control Groups with a VLAN:

Procedure

Step 1 Click **Security** > **ARP Inspection** > **VLAN Settings**.

Step 2 To enable ARP Inspection on a VLAN, move the VLAN from the Available VLANs list to the Enabled VLANs list.

Step 3 To associate an ARP Access Control group with a VLAN, click **Add**. Select the VLAN number and select a previously-defined ARP Access Control Name.

Step 4 Click **Apply**. The settings are defined, and the Running Configuration file is updated.

IPv6 First Hop Security

IPv6 First Hop Security (FHS) is a suite of features designed to secure link operations in an IPv6-enabled network. It is based on the Neighbor Discovery Protocol and DHCPv6 messages.

In this feature, a Layer 2 switch filters Neighbor Discovery Protocol messages, DHCPv6 messages and user data messages according to a number of different rules.

IPv6 First Hop Security Components

IPv6 First Hop Security includes the following features:

- IPv6 First Hop Security Common
- RA Guard
- ND Inspection
- Neighbor Binding Integrity
- DHCPv6 Guard
- IPv6 Source Guard

These components can be enabled or disabled on VLANs. There are two empty, pre-defined policies per each feature with the following names: vlan_default and port_default. The first one is attached to each VLAN that is not attached to a user-defined policy and the second one is connected to each interface and VLAN that is not attached to a user-defined policy.

FHS Settings

Use the FHS Settings page to enable the FHS Common feature on a specified group of VLANs and to set the global configuration value for logging of dropped packets. If required, a policy can be added. The packet drop logging can be added to the system-defined default policy.

To configure IPv6 First Hop Security common parameters:

Procedure

Step 1 Click **Security** > **IPv6 First Hop Security** > **FHS Settings**.

The currently defined policies are displayed. For each policy, its Policy Type is displayed, which indicates whether it's a default or user-defined policy.

Step 2 Enter the following global configuration fields:

- FHS VLAN List—Enter one or more VLANs on which IPv6 First Hop Security is enabled.
- Packet Drop Logging—Select to create a SYSLOG when a packet is dropped by a First Hop Security policy. This is the global default value if no policy is defined.

Step 3 Click **Apply** to add the settings to the Running Configuration file.

Step 4 Create a FHS policy if required by clicking **Add**.

Enter the following fields:

- Policy Name—Enter a user-defined policy name.
- Packet Drop Logging—Select to create a SYSLOG when a packet is dropped as a result of a First Hop Security feature within this policy.
  - Inherited—Use the value from the VLAN or the global configuration.
  - Enable—Create a SYSLOG when a packet is dropped as a result of First Hop Security.
  - Disable—Don't create a SYSLOG when a packet is dropped as a result of First Hop Security.

Step 5 Click **Apply** to add the settings to the Running Configuration file.

Step 6 To attach this policy to an interface:

- Attach Policy to VLAN—Click to jump to Policy Attachment (VLAN), on page 319 page where you can attach this policy to a VLAN.
- Attach Policy to Interface—Click to jump to Policy Attachment (Port), on page 320 page where you can attach this policy to a port.

RA Guard Settings

Use the RA Guard Settings page to enable the RA Guard feature on a specified group of VLANs and to set the global configuration values for this feature. If required, a policy can be added or the system-defined default RA Guard policies can be configured in this page.

To configure RA Guard:

Procedure

Step 1 Click **Security** > **IPv6 First Hop Security** > **RA Guard Settings**.

The currently defined policies are displayed. For each policy, its Policy Type is displayed, which indicates whether it's a default or user-defined policy.

Step 2 Enter the following global configuration field:

- RA Guard VLAN List—Enter one or more VLANs on which RA Guard is enabled.

  Enter the other configuration fields that are described below.

Step 3 To add a policy, click **Add** and enter the fields:

- Policy Name—Enter a user-defined policy name.
- Device Role—Displays one of the following options to specify the role of the device attached to the port for RA Guard.
  - Inherited—Device role is inherited from either the VLAN or system default (client).
  - Host—Device role is host.
  - Router—Device role is router.
- Managed Configuration Flag—This field specifies verification of the advertised Managed Address Configuration flag within an IPv6 RA Guard policy.
  - Inherited—Feature is inherited from either the VLAN or system default (client).
  - No Verification—Disables verification of the advertised Managed Address Configuration flag.
  - On—Enables verification of the advertised Managed Address Configuration flag.
  - Off—The value of the flag must be 0.
- Other Configuration Flag—This field specifies verification of the advertised Other Configuration flag within an IPv6 RA Guard policy.
  - Inherited—Feature is inherited from either the VLAN or system default (client).
  - No Verification—Disables verification of the advertised Other Configuration flag.
  - On—Enables verification of the advertised Managed Other flag.
  - Off—The value of the flag must be 0.

- RA Address List—Specify the list of addresses to filter:
  - Inherited—Value is inherited from either the VLAN or system default (no verification).
  - No Verification—Advertised addresses aren't verified.
  - Match List—IPv6 address list to be matched.
- RA Prefix List—Specify the list of addresses to filter:
  - Inherited—Value is inherited from either the VLAN or system default (no verification).
  - No Verification—Advertised prefixes aren't verified.
  - Match List—Prefix list to be matched.
- Minimal Hop Limit—Indicates if the RA Guard policy checks that the minimum hop limit of the packet received.
  - Inherited—Feature is inherited from either the VLAN or system default (client).
  - No Limit—Disables verification of the lower boundary of the hop count limit.
  - User Defined—Verifies that the hop-count limit is greater than or equal to this value.
- Maximal Hop Limit—Indicates if the RA Guard policy checks that the maximum hop limit of the packet received.
  - Inherited—Feature is inherited from either the VLAN or system default (client).
  - No Limit—Disables verification of the high boundary of the hop-count limit.
  - User Defined—Verifies that the hop-count limit is less than or equal to this value. The value of the high boundary must be equal or greater than the value of the low boundary.
- Minimal Router Preference—This field indicates whether the RA Guard policy verifies the minimum advertised Default Router Preference value in RA messages within an RA Guard policy.
  - Inherited—Feature is inherited from either the VLAN or system default (client).
  - No Verification—Disables verification of the low boundary of Advertised Default Router Preference.
  - Low—Specifies the minimum allowed Advertised Default Router Preference value. The following values are acceptable: low, medium, and high (see RFC4191).
  - Medium—Specifies the minimum allowed Advertised Default Router Preference value. The following values are acceptable: low, medium, and high (see RFC4191).
  - High—Specifies the minimum allowed Advertised Default Router Preference value. The following values are acceptable: low, medium, and high (see RFC4191).
- Maximal Router Preference—This field indicates whether the RA Guard policy verifies the maximum advertised Default Router Preference value in RA messages within an RA Guard policy.
  - Inherited—Feature is inherited from either the VLAN or system default (client).
  - No Verification—Disables verification of the high boundary of Advertised Default Router Preference.
  - Low—Specifies the maximum allowed Advertised Default Router Preference value. The following values are acceptable: low, medium, and high (see RFC4191).

- Medium—Specifies the maximum allowed Advertised Default Router Preference value. The following values are acceptable: low, medium, and high (see RFC4191).
- High—Specifies the maximum allowed Advertised Default Router Preference value. The following values are acceptable: low, medium, and high (see RFC4191).

Step 4 Click **Apply** to add the settings to the Running Configuration file.

Step 5 To configure system-defined default policies or existing user defined policy select the policy in the policy table and click **Edit.**

Step 6 To attach this policy to an interface:

- Attach Policy to VLAN—Click to jump to Policy Attachment (VLAN), on page 319 page where you can attach this policy to a VLAN.
- Attach Policy to Interface—Click to jump to Policy Attachment (Port), on page 320 page where you can attach this policy to a port.

DHCPv6 Guard Settings

Use the DHCPv6 Guard Settings page to enable the DHCPv6 Guard feature on a specified group of VLANs and to set the global configuration values for this feature. If required, a policy can be added or the system-defined default DHCPv6 Guard policies can be configured in this page.

To configure DHCPv6 Guard:

Procedure

Step 1 Click **Security** > **IPv6 First Hop Security** > **DHCPv6 Guard Settings**.

The currently defined policies are displayed. For each policy, its Policy Type is displayed, which indicates whether it's a default or user-defined policy.

Step 2 Enter the following global configuration fields:

- DHCPv6 Guard VLAN List—Enter one or more VLANs on which DHCPv6 Guard is enabled.
- Device Role—Displays the device role. See definition in the Add page.
- Minimal Preference—This field indicates whether the DHCPv6 Guard policy checks the minimum advertised preference value of the packet received.
  - No Verification—Disables verification of the minimum advertised preference value of the packet received.
  - User Defined—Verifies that the advertised preference value is greater than or equal to this value. This value must be less than the Maximal Preference value.
- Maximal Preference—This field indicates whether the DHCPv6 Guard policy checks the maximum advertised preference value of the packet received. This value must be greater than the Minimal Preference value.
  - No Verification—Disables verification of the lower boundary of the hop count limit.

- User Defined—Verifies that the advertised preference value is less than or equal to this value.

Step 3 Click **Apply** to add the settings to the Running Configuration file.

The existing policies are displayed. The fields are displayed below except for the Policy Type field. This displays whether the policy is user-defined or a default one.

Step 4 If required, click **Add** to create a DHCPv6 policy.

Step 5 Enter the following fields:

- Policy Name—Enter a user-defined policy name.
- Device Role—Select either Server or Client to specify the role of the device attached to the port for DHCPv6 Guard.
  - Inherited—Role of device is inherited from either the VLAN or system default (client).
  - Client—Role of device is client.
  - Server—Role of device is server.
- Match Reply Prefixes—Select to enable verification of the advertised prefixes in received DHCP reply messages within a DHCPv6 Guard policy.
  - Inherited—Value is inherited from either the VLAN or system default (no verification).
  - No Verification—Advertised prefixes aren’t verified.
  - Match List—IPv6 prefix list to be matched.
- Match Server Address—Select to enable verification of the DHCP server's and relay’s IPv6 address in received DHCP reply messages within a DHCPv6 Guard policy.
  - Inherited—Value is inherited from either the VLAN or system default (no verification).
  - No Verification—Disables verification of the DHCP server's and relay’s IPv6 address.
  - Match List— IPv6 prefix list to be matched.
- Minimal Preference—This field indicates whether the DHCPv6 Guard policy checks the minimum advertised preference value of the packet received.
  - Inherited—Minimal preference is inherited from either the VLAN or system default (client).
  - No Verification—Disables verification of the minimum advertised preference value of the packet received.
  - User Defined—Verifies that the advertised preference value is greater than or equal to this value. This value must be less than the Maximal Preference value.
- Maximal Preference—This field indicates whether the DHCPv6 Guard policy checks the maximum advertised preference value of the packet received. This value must be greater than the Minimal Preference value.
  - Inherited—Minimal preference is inherited from either the VLAN or system default (client).
  - No Verification—Disables verification of the lower boundary of the hop count limit.
  - User Defined—Verifies that the advertised preference value is less than or equal to this value.

Step 6 Click **Apply** to add the settings to the Running Configuration file.

Step 7 To attach this policy to an interface:

- Attach Policy to VLAN—Click to jump to Policy Attachment (VLAN), on page 319 page where you can attach this policy to a VLAN.
- Attach Policy to Interface—Click to jump to Policy Attachment (Port), on page 320 page where you can attach this policy to a port.

ND Inspection Settings

Use the Neighbor Discovery (ND) Inspection Settings page to enable the ND Inspection feature on a specified group of VLANs and to set the global configuration values for this feature. If required, a policy can be added or the system-defined default ND Inspection policies can be configured in this page.

To configure ND Inspection:

Procedure

Step 1 Click **Security** > **IPv6 First Hop Security** > **ND Inspection Settings**.

The existing policies are displayed. The fields are displayed below except for the Policy Type field. This displays whether the policy is user-defined or a default one.

Step 2 Enter the following global configuration fields:

- ND Inspection VLAN List—Enter one or more VLANs on which ND Inspection is enabled.
- Device Role—Displays the device role that is explained below.
- Drop Unsecure—Select to enable dropping messages with no CGA or RSA Signature option within an IPv6 ND Inspection policy.
- Minimal Security Level—If unsecure messages aren't dropped, select the security level below which messages aren't forwarded.
  - No Verification—Disables verification of the security level.
  - User Defined—Specify the security level of the message to be forwarded.
- Validate Source MAC—Select to globally enable checking source MAC address against the link-layer address.

Step 3 Click **Apply** to add the settings to the Running Configuration file.

Step 4 If required, click **Add** to create an ND Inspection policy.

Step 5 Enter the following fields:

- Policy Name—Enter a user-defined policy name.
- Device Role—Select one of the following to specify the role of the device attached to the port for ND Inspection.
  - Inherited—Role of device is inherited from either the VLAN or system default (client).

- Host—Role of device is host.
- Router—Role of device is router.

- Drop Unsecure—Select one of following options:
  - Inherited—Inherit value from VLAN or system default (disabled).
  - Enable—Enable dropping messages with no CGA or RSA Signature option within an IPv6 ND Inspection policy.
  - Disable—Disable dropping messages with no CGA or RSA Signature option within an IPv6 ND Inspection policy.
- Minimal Security Level—If unsecure messages aren't dropped, select the security level below which messages aren't forwarded.
  - Inherited—Inherit value from VLAN or system default (disabled).
  - No Verification—Disables verification of the security level.
  - User Defined—Specify the security level of the message to be forwarded.
- Validate Source MAC—Specify whether to globally enable checking source MAC address against the link-layer address:
  - Inherited—Inherit value from VLAN or system default (disabled).
  - Enable—Enable checking source MAC address against the link-layer address.
  - Disable—Disable checking source MAC address against the link-layer address.

Step 6 Click **Apply** to add the settings to the Running Configuration file.

Step 7 To attach this policy to an interface:

- Attach Policy to VLAN— To attach this policy to a VLAN, jump to Policy Attachment (VLAN), on page 319 .
- Attach Policy to Interface—To attach this policy to an interface, jump to Policy Attachment (Port), on page 320

Neighbor Binding Settings

The Neighbor Binding table is a database table of IPv6 neighbors connected to a device is created from information sources, such as Neighbor Discovery Protocol (NDP) snooping. This database, or binding, table is used by various IPv6 guard features to prevent spoofing and redirect attacks.

Use the Neighbor Binding Settings page to enable the Neighbor Binding feature on a specified group of VLANs and to set the global configuration values for this feature. If required, a policy can be added or the system-defined default Neighbor Binding policies can be configured in this page.

To configure Neighbor Binding:

Procedure

Step 1 Click **Security** > **IPv6 First Hop Security** > **Neighbor Binding Settings**.

Step 2 Enter the following global configuration fields:

Neighbor Binding VLAN List	Enter one or more VLANs on which Neighbor Binding is enabled.
Device Role	Displays the device global default role (Perimeter).
Neighbor Binding Lifetime	Enter the length of time that addresses remain in the Neighbor Bindings table.
Neighbor Binding Logging	Select to enable logging of Neighbor Binding table main events.
Address Prefix Validation	Select to enable IPv6 Source Guard validation of addresses.

Global Address Binding Configuration

Binding from NDP Messages	To change the global configuration of allowed configuration methods of global IPv6 addresses within an IPv6 Neighbor Binding policy, select one of the following options: • Any—Any configuration methods (stateless and manual) are allowed for global IPv6 bound from NDP messages. • Stateless—Only stateless auto configuration is allowed for global IPv6 bound from NDP messages. • Disable—Binding from NDP messages is disabled.
Binding from DHCPv6 Messages	Binding from DHCPv6 is allowed.

Neighbor Binding Entry Limits

Entries per VLAN	Select **Inherited** to use global value, No Limit to set no limit on the number of entries and User Defined to set a special value for this policy.
Entries per Interface	Select **Inherited** to use global value, No Limit to set no limit on the number of entries and User Defined to set a special value for this policy.
Entries per MAC Address	Select **Inherited** to use global value, No Limit to set no limit on the number of entries and User Defined to set a special value for this policy.

Step 3 Click **Apply** to add the settings to the Running Configuration file.

Step 4 If required, click **Add** to create a Neighbor Binding policy.

Step 5 Enter the following fields:

Policy Name	Enter a user-defined policy name.

Device Role	Select **one of** the following options to specify the role of the device attached to the port for the Neighbor Binding policy. • Inherited—Role of device is inherited from either the VLAN or system default (client). • Perimeter—Port is connected to devices not supporting IPv6 First Hop Security. • Internal—Port is connected to devices supporting IPv6 First Hop Security.
Neighbor Binding Logging	Select one of the following options to specify logging: • Inherited—Logging option is the same as the global value. • Enable—Enable logging of Binding table main events. • Disable—Disable logging of Binding table main events.
Address Prefix Validation	Select one of the following options to specify validation of addresses: • Inherited—Validation option is the same as the global value. • Enable—Enable validation of addresses. • Disable—Disable validation of addresses

Global Address Binding Configuration

Inherit Address Binding Settings	Enable to use the global address binding settings.
Binding from NDP Messages	To change the global configuration of allowed configuration methods of global IPv6 addresses within an IPv6 Neighbor Binding policy, select one of the following options: • Any—Any configuration methods (stateless and manual) are allowed for global IPv6 bound from NDP messages. • Stateless—Only stateless auto configuration is allowed for global IPv6 bound from NDP messages. • Disable—Binding from NDP messages is disabled.
Binding from DHCPv6 Messages	Select to enable binding from DHCPv6.

Neighbor Binding Entry Limits

Entries per VLAN	Select **Inherited** to use global value, No Limit to set no limit on the number of entries and User Defined to set a special value for this policy.
Entries per Interface	Select **Inherited** to use global value, No Limit to set no limit on the number of entries and User Defined to set a special value for this policy.
Entries per MAC Address	Select **Inherited** to use global value, No Limit to set no limit on the number of entries and User Defined to set a special value for this policy.

Step 6 Click **Apply** to add the settings to the Running Configuration file.

Step 7 To attach this policy to an interface:

Attach Policy to VLAN	Click to jump to Policy Attachment (VLAN), on page 319 page where you can attach this policy to a VLAN.
Attach Policy to Interface	Click to jump to Policy Attachment (Port), on page 320 page where you can attach this policy to a port.

IPv6 Source Guard Settings

Use the IPv6 Source Guard Settings page to enable the IPv6 Source Guard feature on a specified group of VLANs. If required, a policy can be added or the system-defined default IPv6 Source Guard policies can be configured in this page.

To configure IPv6 Source Guard:

Procedure

Step 1 Click **Security** > **IPv6 First Hop Security** > **IPv6 Source Guard Settings**.

The existing policies are displayed. The fields are displayed below except for the Policy Type field. This displays whether the policy is user-defined or a default one.

Step 2 Enter the following global configuration fields:

- IPv6 Source Guard VLAN List—Enter one or more VLANs on which IPv6 Source Guard is enabled.
- Port Trust—Displays that by default the policies are for untrusted ports. This can be changed per policy.

Step 3 If required, click **Add** to create a First Hop Security policy.

Step 4 Enter the following fields:

- Policy Name—Enter a user-defined policy name.
- Port Trust—Select the port trust status of the policy:
  - Inherited—When policy is attached to a port it's untrusted).
  - Trusted—When policy is attached to a port it's trusted.

Step 5 Click **Apply** to attach the policy.

Step 6 To attach this policy to an interface click **Attach Policy to Interface.**

Policy Attachment (VLAN)

To attach a policy to one or more VLANs:

Procedure

Step 1 Click **Security** > **IPv6 First Hop Security** > **Policy Attachment (VLAN)**.

The list of policies that are already attached are displayed along with their Policy Type, Policy Name and VLAN List.

Step 2 To attach a policy to a VLAN, click **Add** and enter the following fields:

- Policy Type—Select the policy type to attach to the interface.
- Policy Name—Select the name of the policy to attach to the interface.
- VLAN List—Select the VLANs to which the policy is attached.

Step 3 Click **Apply** to add the settings to the Running Configuration file.

Policy Attachment (Port)

To attach a policy to one or more ports or LAGs:

Procedure

Step 1 Click **Security** > **IPv6 First Hop Security** > **Policy Attachment (Port)**.

The list of policies that are already attached are displayed along with their Interface, Policy Type, Policy Name and VLAN List.

Step 2 To attach a policy to a port or LAG, click **Add** and enter the following fields:

- Interface—Select the interface on which the policy will be attached.
- Policy Type—Select the policy type to attach to the interface.
- Policy Name—Select the name of the policy to attach to the interface.
- VLAN List—Select the VLANs to which the policy is attached.

Step 3 Click **Apply** to add the settings to the Running Configuration file.

Neighbor Binding Table

To view entries in the Neighbor Binding table:

Procedure

Step 1 Click **Security** > **IPv6 First Hop Security** > **Neighbor Binding Table**

Step 2 Select one of the following clear table options:

- Static Only—Clear all static entries in the table.
- Dynamic Only—Clear all dynamic entries in the table.
- All Dynamic & Static—Clear all dynamic and static entries in the table.

The following fields are displayed for each policy (only fields not on Add page are displayed:

- Origin—Protocol that added the IPv6 address (only available for dynamic entries):
  - Static—Added manually.
  - NDP—Learnt from Neighbor Discovery Protocol messages
  - DHCP—Learnt from DHCPv6 protocol messages
- State—State of the entry:
  - Tentative—The new host IPv6 address is under validation. Since its lifetime is less than 1 sec its expiration time isn't displayed.
  - Valid—The host IPv6 address was bound.
- Expiry Time (Sec.)—Remaining time in seconds until the entry will be removed, if it's not confirmed.
- TCAM Overflow—Entries marked as No don't have a TCAM overflow.

Step 3 To add a policy, click **Add** and enter the following fields:

- VLAN ID—VLAN ID of the entry.
- IPv6 Address—Source IPv6 address of the entry.
- Interface—Port on which packet is received.
- MAC Address—Neighbor MAC address of the packet.

Step 4 Click **Apply** to add the settings to the Running Configuration file.

Neighbor Prefix Table

You can add static prefixes for global IPv6 addresses bound from NDP messages in the Neighbor Prefix table. Dynamic entries are learned.

To add entries to the Neighbor Prefix table:

Procedure

Step 1 Click **Security** > **IPv6 First Hop Security** > **Neighbor Prefix Table.**

Step 2 Select one of the following options in the Clear Table field to clear the Neighbor Prefix table:

- Static Only—Clear only static entries.
- Dynamic Only—Clear only dynamic entries.
- All Dynamic & Static—Clear static and dynamic entries.

Step 3 The following fields are displayed for the exiting entries:

- VLAN ID—VLAN on which the prefixes are relevant.
- IPv6 Prefix—IPv6 prefix.
- Prefix Length—IPv6 prefix length.
- Origin—Entry is dynamic (learned) or static (manually configured).
- Autoconfig—The prefix can be used for stateless configuration.
- Expiry Time (Sec)—Length of time entry remains before being deleted.

Step 4 Click **Add** to add a new entry to the table and enter the above fields for the new entry.

FHS Status

To display the global configuration for the FHS features:

Procedure

Step 1 Click **Security** > **IPv6 First Hop Security** > **FHS Status.**

Step 2 Select a port, LAG or VLAN for which the FHS state is reported.

Step 3 The following fields are displayed for the selected interface:

FHS Status

FHS State on Current VLAN	Is FHS enabled on the current VLAN
Packet Drop Logging	Is this feature enabled for the current interface (at the level of global configuration or in a policy attached to the interface)

RA Guard Status

RA Guard State on Current VLAN	Is RA Guard enabled on the current VLAN?

Device Role	RA device role.
Managed Configuration Flag	Is verification of the managed configuration flag enabled?
Other Configuration Flag	Is verification of the other configuration flag enabled?
RA Address List	RA address list to be matched.
RA Prefix List	RA prefix list to be matched.
Minimal Hop Limit	Is minimum RA hop limit verification enabled?
Maximal Hop Limit	Is maximum RA hop limit verification enabled?
Minimal Router Preference	Is minimum router preference verification enabled?
Maximal Router Preference	Is maximum router preference verification enabled?

DHCPv6 Guard Status

DHCPv6 Guard State on Current VLAN	Is DHCPv6 Guard enabled on the current VLAN?
Device Role	DHCP device role
Match Reply Prefixes	Is DHCP reply prefixes verification enabled?
Match Server Address	Is DHCP server addresses verification enabled?
Minimal Preference	Is verification of the minimal preference enabled?
Maximal Preference	Is verification of the maximum preference enabled?

ND Inspection Status

ND Inspection State on Current VLAN	Is ND Inspection enabled on the current VLAN?
Device Role	ND Inspection device role.
Drop Unsecure	Are unsecure messages dropped?
Minimal Security Level	If unsecure messages aren’t dropped, what is the minimum security level for packets to be forwarded?
Validate Source MAC	Is source MAC address verification enabled?

Neighbor Binding Status

Neighbor Binding State on Current VLAN	Is Neighbor Binding enabled on the current VLAN?
Device Role	Neighbor Binding device role.
Logging Binding	Is logging of Neighbor Binding table events enabled?

Address Prefix Validation	Is address prefix validation enabled?
Global Address Configuration	Which messages are validated?
Max Entries per VLAN	Maximum number of dynamic Neighbor Binding table entries per VLAN allowed.
Max Entries per Interface	Maximum number of Neighbor Binding table entries per interface allowed.
Max Entries per MAC Address	Maximum number of Neighbor Binding table entries per MAC address allowed.

IPv6 Source Guard Status

IPv6 Source Guard State on Current VLAN	Is IPv6 Source Guard enabled on the current VLAN?
Port Trust	Whether the port is trusted and how it received its trusted status.

FHS Statistics

To display FHS statistics:

Procedure

Step 1 Click **Security** > **IPv6 First Hop Security** > **FHS Statistics.**

Step 2 Select the Refresh Rate, the time period that passes before the statistics are refreshed.

Step 3 The following global overflow counters are displayed:

Neighbor Binding Table	Number of entries that could not be added to this table because the table reached its maximum size.
Neighbor Prefix Table	Number of entries that could not be added to this table because the table reached its maximum size.
TCAM	Number of entries that could not be added because of TCAM overflow.

Step 4 Select an interface and the following fields are displayed:

NDP (Neighbor Discovery Protocol) Messages	The number of received and dropped messages are displayed for the following types of messages: • RA—Router Advertisement messages • REDIR—Redirect messages • NS—Neighbor Solicitation messages. • NA—Neighbor Advertisement messages. • RS—Router Solicitation message.
DHCPv6 Messages	The number of received and dropped messages are displayed for the following types of DHCPv6 messages: • ADV— Advertise messages • REP—Reply messages • REC—Reconfigure messages • REL-REP—Relay reply messages • LEAS-REP—Lease query reply messages • RLS—Released messages • DEC—Decline messages

The following fields are displayed in the FHS Dropped Message Table

Feature	Type of message dropped (DHCPv6 Guard, RA Guard and so on).
Count	Number of messages dropped.
Reason	Reason that the messages dropped.

Step 5 Click **Clear Interface Counters** or **Clear All Interface Counters** or **Clear Global Counters** to clear the counters.

Step 6 Click **Refresh** to refresh the counters.

Certificate Settings

The Cisco Business Dashboard Probe (CBD) and Plug-n-Play (PNP) features require CA certificates to establish HTTPS communication with the CBD or PNP servers. The Certificate Settings feature allows these applications and device managers to do the following:

- Install trusted CA certificates and to remove certificates that are no longer wanted
- Statically add certificates to device configuration file
- Manage a revocation list of untrusted certificates

Note The validity of the certificates is based on the system clock. Use the default system clock or it does not provide proper validation. Therefore, make sure the system clock is based on device Real time clock (if supported) or was actively set since the last reboot (preferably via SNTP service). If the system clock is not based on RTC or was not set since last reboot validation of certificate will fail, even if the system clock is within the validity date of the certificate.

Dynamic Certificates

The CBD and PNP applications can install dynamic trusted certificates to the device memory. The installed certificate must include the following attributes:

- Certificate name - A string that is used to identify the certificate.
- Owner - The application name that installed the certificate (for example, PNP, CBD)
- The certificate itself in PEM format.

An application can also delete a specific or all dynamic certificates installed by that application.

Considerations

- Up to 512 dynamic certificates can be installed on the device.
- Dynamic certificates are removed when the device reboots

Static Certificates

If an application wants to add a certificate that will not be deleted on reset, or if a user of the switch wants to add a certificate, they can add a static certificate. These certificates are saved in the device running configuration and can be copied to the startup configuration.

Adding a static certificate requires providing the following attributes:

- Certificate name - This is a string that is used to identify the certificate.
- Owner - the name of the application that installed the certificate (for example, PNP, CBD), or "static" if certificate is added by a user.
- The certificate itself in PEM format.

Considerations

- Up to 256 static certificates can be installed on the device.
- It is possible for identical certificates to be added by different applications or users as long as the names used to identify them are different.

CA Certificate Setting

Users can access information on all installed certificates (dynamic and static). The following information is displayed per each certificate:

Procedure

Step 1 Click **Security** > **Certificate Settings** > **CA Certificate Settings**.

Step 2 To import a new certificate, click **Add** and complete the following:

- Certificate Name—Enter the name of the certificate.
- Certificate—Paste the certificate in PEM format (including the begin and end marker lines).

Step 3 Click **Apply** to apply the new settings.

Step 4 To view the details of an existing certificate, select the certificate from the list and click **Details**. The following will be displayed:

Option	Description
Certificate Name	The name or unique identifier of the certificate.
Type	This can be signer, static or dynamic.
Owner	This can be signer, static, CBD or PNP
Version	The version of the certificate.
Serial Number	The serial number of the certificate.
Status	The status of the certificate.
Valid From	The date and time from which certificate is valid,
Valid To	The date and time until which the certificate is valid.
Issuer	The entity or CA that signed the certificate.
Subject	Distinguished name (DN) information for the certificate.
Public Key Type	The type of the public key.
Public Key Length	The length (in bits) of the public key.
Signature Algorithm	The cryptographic algorithm used by the CA to sign the certificate.
Certificate	The certificate details in PEM format.

Step 5 You can use the following filters to find a specific certificate.

- Type equals to—Check this box and select Signer, Static, or Dynamic from the drop-down list, to filter by these certificate types.
- Owner equals to—Paste the certificate in PEM format (including the begin and end marker lines).

Step 6 To remove one or more certificates select the certificate(s) and press **Delete**. Only Static certificates can be deleted.

CA Revocation List

If a certificate becomes untrusted for any reason, it can be added to the revocation list by the user or one of the applications. If a certificate is included in the revocation list, it is considered non-valid and the device will not allow it to be used. Adding a certificate to the revocation list will not remove the revoked certificate from the certificate database. It will only update its status to Not Valid (Revoked). When a certificate is removed from the revocation list, its status is automatically updated in the certificate database. There is no need to re-install it.

To add or remove a certificate to/from the revocation list, complete the following:

Procedure

Step 1 Click **Security** > **Certificate Settings** > **CA Certificate Revocation List**.

Step 2 Click **Add** to open the Add Revoked Certificate dialog box

Step 3 Provide the following details:

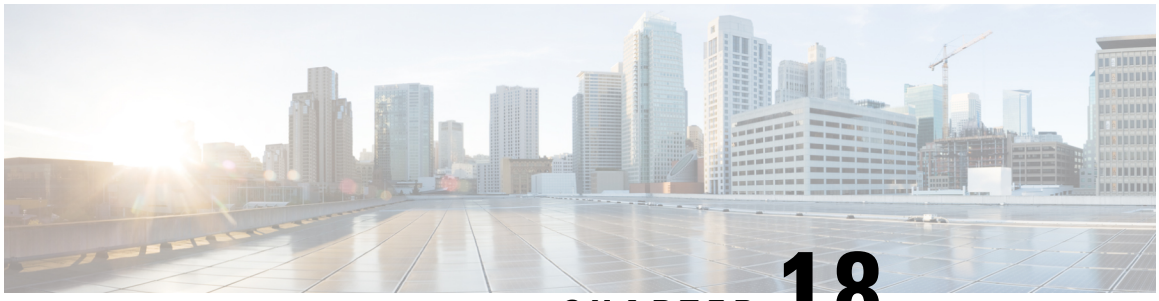
- Issuer—The string identifying the issuer (for example: "C=US, O=MyTrustOrg, CN=MyCommonName") (0-160 chars).
- Serial Number—The serial number of the revoked certificate. This is a string of hexadecimal pairs (length 2-40).

Step 4 Click **Apply** to add the certificate.

Considerations

- Up to 512 certificates can be added to the revocation list.
- All certificates that match the entry in the revocation list are considered not valid (even if they are identified under different names in the certificate database).

Step 5 To delete an existing certificate, select the certificate from the Revoked CA Certificate Table and click **Delete**.



CHAPTER 18

Access Control

The Access Control List (ACL) feature is part of the security mechanism. ACL definitions serve as one of the mechanisms to define traffic flows that are given a specific Quality of Service (QoS). For more information see Quality of Service. ACLs enable network managers to define patterns (filter and actions) for ingress traffic. Packets, entering the device on a port or LAG with an active ACL, are either admitted or denied entry. This chapter contains the following sections:

- MAC-Based ACL, on page 329
- MAC-based ACE, on page 330
- IPv4-based ACL, on page 331
- IPv4-Based ACE, on page 331
- IPv6-Based ACL, on page 335
- IPv6-Based ACE, on page 336
- ACL Binding (VLAN), on page 338
- ACL Binding (Port), on page 339

MAC-Based ACL

MAC-based ACLs are used to filter traffic based on Layer 2 fields. MAC-based ACLs check all frames for a match. To define a MAC-based ACL follow these steps:

Procedure

Step 1 Click **Access Control** > **MAC-Based ACL**.

This page contains a list of all currently defined MAC-based ACLs.

Step 2 Click **Add**.

Step 3 Enter the name of the new ACL in the ACL Name field. ACL names are case-sensitive.

Step 4 Click **Apply**. The MAC-based ACL is saved to the Running Configuration file.

MAC-based ACE

Note Each MAC-based rule consumes one TCAM rule. The TCAM allocation is performed in couples, such that, for the first ACE, 2 TCAM rules are allocated and the second TCAM rule is allocated to the next ACE, and so forth.

To add rules (ACEs) to an ACL, complete the following steps:

Procedure

Step 1 Click **Access Control** > **Mac-Based ACE**.

Step 2 Select an ACL, and click **Go**. The ACEs in the ACL are listed.

Step 3 Click **Add**.

Step 4 Enter the parameters.

- ACL Name—Displays the name of the ACL to which an ACE is being added.
- Priority—Enter the priority of the ACE. ACEs with higher priority are processed first. One is the highest priority.
- Action—Select the action taken upon a match. The options are:
  - Permit—Forward packets that meet the ACE criteria.
  - Deny—Drop packets that meet the ACE criteria.
  - Shutdown—Drop packets that meet the ACE criteria, and disable the port from where the packets received.
- Logging—Select to enable logging ACL flows that match the ACL rule.
- Time Range—Select to enable limiting the use of the ACL to a specific time range.
- Time Range Name—If Time Range is selected, select the time range to be used. Click **Edit** to revise the time range.
- Destination MAC Address—Select Any if all destination addresses are acceptable or User defined to enter a destination address or a range of destination addresses.
- Destination MAC Address Value—Enter the MAC address to which the destination MAC address is to be matched and its mask (if relevant).
- Destination MAC Wildcard Mask—Enter the mask to define a range of MAC addresses. This mask is different than in other uses, such as subnet mask. Here, setting a bit as 1 indicates don't care and 0 indicates to match that value.

  Note
  Given a mask of 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1111 1111 (which means that you match on the bits where there are 0's and ignore the bits where there are 1's): You need to translate the binary value to hexadecimal (four bits per hex digit). In this example, since 1111 1111 = FF, the mask would be written as 00:00:00:00:00:FF.

- Source MAC Address—Select Any if all source addresses are acceptable or User defined to enter a source address or range of source addresses.
- Source MAC Address Value—Enter the MAC address to which the source MAC address is to be matched and its mask (if relevant).
- Source MAC Wildcard Mask—Enter the mask to define a range of MAC addresses.
- VLAN ID—Enter the VLAN ID section of the VLAN tag to match.
- 802.1p—Select **Include** to use 802.1p.
- 802.1p Value—Enter the 802.1p value to be added to the VPT tag.
- 802.1p Mask—Enter the wildcard mask to be applied to the VPT tag.
- Ethertype—Enter the frame Ethertype to be matched.

Step 5 Click **Apply**. The MAC-based ACE is saved to the Running Configuration file.

IPv4-based ACL

ACLs are also used as the building elements of flow definitions for per-flow QoS handling. IPv4-based ACLs are used to check IPv4 packets. To define an IPv4-based ACL, follow these steps:

Procedure

Step 1 Click **Access Control** > **IPv4-Based ACL**.

This page contains all currently defined IPv4-based ACLs.

Step 2 Click **Add**.

Step 3 Enter the name of the new ACL in the ACL Name field. The names are case-sensitive.

Step 4 Click **Apply**. The IPv4-based ACL is saved to the Running Configuration file.

IPv4-Based ACE

Note Each IPv4-based rule consumes one TCAM rule. The TCAM allocation is performed in couples, such that, for the first ACE. Two TCAM rules are allocated and the second TCAM rule is allocated to the next ACE, and so forth.

To add rules (ACEs) to an IPv4-based ACL, follow these steps:

Procedure

Step 1 Click **Access Control** > **IPv4-Based ACE**.

Step 2 Select an ACL, and click **Go**. All currently-defined IP ACEs for the selected ACL are displayed.

Step 3 Click **Add**.

Step 4 Enter the parameters.

ACL Name	Displays the name of the ACL to which an ACE is being added.
Priority	Enter the priority. ACEs with higher priority are processed first.
Action	Select the action assigned to the packet matching the ACE from the following options: • Permit—Forward packets that meet the ACE criteria. • Deny—Drop packets that meet the ACE criteria. • Shutdown—Drop packets that meet the ACE criteria, and disable the port to which the packets addressed. Ports are reactivated on the Error Recovery Settings, on page 122 page.
Logging	Select to enable logging ACL flows that match the ACL rule.
Time Range	Select to enable limiting the use of the ACL to a specific time range
Time Range Name	If Time Range is selected, click the Edit button to be redirected to the time range page and select the time range name to be used. Time ranges are described in the System Time, on page 64 section.

Protocol	Select to create an ACE based on a specific protocol or protocol ID. Select Any (IPv4) to accept all IP protocols. Otherwise select one of the following protocols: • ICMP—Internet Control Message Protocol • IGMP—Internet Group Management Protocol • IP in IP—IP in IP encapsulation • TCP—Transmission Control Protocol • EGP—Exterior Gateway Protocol • IGP—Interior Gateway Protocol • UDP—User Datagram Protocol • HMP—Host-Mapping Protocol • RDP—Reliable Datagram Protocol. • IDPR—Inter-Domain Policy Routing Protocol • IPV6—IPv6 over IPv4 tunneling • IPV6:ROUT—Matches packets belonging to the IPv6 over IPv4 route through a gateway • IPV6:FRAG—Matches packets belonging to the IPv6 over IPv4 Fragment Header • IDRP—Inter-Domain Routing Protocol • RSVP—ReSerVation Protocol • AH—Authentication Header • IPV6:ICMP—Internet Control Message Protocol • EIGRP—Enhanced Interior Gateway Routing Protocol • OSPF—Open Shortest Path First • IPIP—IP in IP • PIM—Protocol Independent Multicast • L2TP—Layer 2 Tunneling Protocol • ISIS—IGP-specific protocol • Protocol ID to Match—Instead of selecting the name, enter the protocol ID.
Source IP Address	Select Any if all source addresses are acceptable or User defined to enter a source address or range of source addresses.
Source IP Address Value	Enter the IP address to which the source IP address is to be matched and its mask (if relevant).

Source IP Wildcard Mask	Enter the mask to define a range of IP addresses. This mask is different than in other uses, such as subnet mask. Here, setting a bit as 1 indicates don't care and 0 indicates to mask that value. **Note** Given a mask of 0000 0000 0000 0000 0000 0000 1111 1111, you need to translate the 1's to a decimal integer and you write 0 for every four zeros. In this example since 1111 1111 = 255, the mask would be written: as 0.0.0.255.
Destination IP Address	Select Any if all destination addresses are acceptable or User defined to enter a destination address or a range of destination addresses.
Destination IP Address Value	Enter the IP address to which the destination MAC address is matched and its mask (if relevant).
Destination IP Wildcard Mask	Enter the destination IP wildcard mask.
Source Port	Select one of the following • Any—Match to all source ports. • Single from list—Select a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is selected in the IP Protocol drop-down menu. • Single by number—Enter a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is selected in the IP Protocol drop-down menu. • Range—Enter a range from 0 - 65535.
Destination Port	Select one of the available values. They are the same as for the Source Port field described above. **Note** You must specify the IPv6 protocol for the ACL before you can configure the source and/or destination port.
TCP Flags	Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. For each type of flag, select one of the following options: • Set—Match if the flag is SET. • Unset—Match if the flag is Not SET. • Don’t care—Ignore the TCP flag.

Type of Service	The service type of the IP packet. • Any—Any service type • DSCP to match—Differentiated Serves Code Point (DSCP) to match. • IP Precedence to match—IP precedence is a model of TOS (type of service) that the network uses to help provide the appropriate QoS commitments. This model uses the 3 most significant bits of the service type byte in the IP header, as described in RFC 791 and RFC 1349.
ICMP	If the ACL is based on ICMP, select the ICMP message type that is used for filtering purposes. Either select the message type by name or enter the message type number. If all message types are accepted, select Any. • Any—All message types are accepted. • Select from list—Select message type by name from the drop-down list. • ICMP Type to Match—Number of message types that is to be used for filtering purposes.
ICMP Code	The ICMP messages may have a code field that indicates how to handle the message. Select one of the following options, to configure whether to filter on this code: • Any—Accept all codes. • User Defined—Enter an ICMP code for filtering purposes.
IGMP	If the ACL is based on IGMP, select the IGMP message type to be used for filtering purposes. Either select the message type by name or enter the message type number: • Any—All message types are accepted. • Select from list—Select message type by name. • IGMP Type to match—Number of message type that is to be used for filtering purposes.

Step 5 Click **Apply**. The IPv4-based ACE is saved to the Running Configuration file.

IPv6-Based ACL

The IPv6 based ACL check the IPv6-based traffic. ACLs are also used as the building elements of flow definitions for per-flow QoS handling. To define an IPv6-based ACL, follow these steps:

Procedure

Step 1 Click **Access Control** > **IPv6-Based ACL**.

This window contains the list of defined ACLs and their contents.

Step 2 Click **Add**.

Step 3 Enter the name of a new ACL in the ACL Name field. The names are case-sensitive.

Step 4 Click **Apply**. The IPv6-based ACL is saved to the Running Configuration file.

IPv6-Based ACE

Note Each IPv6-based rule consumes two TCAM rules.

To define an IPv6-based ACL, follow these steps:

Procedure

Step 1 Click **Access Control** > **IPv6-Based ACE**.

This window contains the ACE (rules) for a specified ACL (group of rules).

Step 2 Select an ACL, and click **Go**. All currently-defined IP ACEs for the selected ACL are displayed.

Step 3 Click **Add**.

Step 4 Enter the parameters.

ACL Name	Displays the name of the ACL to which an ACE is being added.
Priority	Enter the priority. ACEs with higher priority are processed first.
Action	Select the action assigned to the packet matching the ACE from the following options: • Permit—Forward packets that meet the ACE criteria. • Deny—Drop packets that meet the ACE criteria. • Shutdown—Drop packets that meet the ACE criteria, and disable the port to which the packets addressed. Ports are reactivated on the Error Recovery Settings, on page 122 page.
Logging	Select to enable logging ACL flows that match the ACL rule.
Time Range	Select to enable limiting the use of the ACL to a specific time range
Time Range Name	If Time Range is selected, click the Edit button to be redirected to the time range page and select the time range name to be used. Time ranges are described in the System Time, on page 64 section.

Protocol	Select to create an ACE based on a specific protocol from the following options: • Any (IPv6)—All source IPv6 addresses apply to the ACE • TCP—Transmission Control Protocol Enables two hosts to communicate and exchange data streams TCP guarantees packet delivery, and guarantees that packets are transmitted and received in the order they sent. • UDP—User Datagram Protocol Transmits packets but doesn't guarantee their delivery. • ICMP—Matches packets to the Internet Control Message Protocol (ICMP). Or • Protocol ID to Match—Enter the ID of the protocol to be matched.
Source IP Address	Select Any if all source addresses are acceptable or User defined to enter a source address or range of source addresses.
Source IP Address Value	Enter the IP address to which the source IP address is to be matched and its mask (if relevant).
Source IP Prefix Length	Enter the prefix length of the source IP address.
Destination IP Address	Select Any if all destination addresses are acceptable or User defined to enter a destination address or a range of destination addresses.
Destination IP Address Value	Enter the IP address to which the destination MAC address is matched and its mask (if relevant).
Destination IP Prefix Length	Enter the prefix length of the IP address.
Source Port	Select one of the following • Any—Match to all source ports. • Single from list—Select a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is selected in the IP Protocol drop-down menu. • By number—Enter a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is selected in the IP Protocol drop-down menu.
Destination Port	Select one of the available values. They are the same as for the Source Port field described above. **Note** You must specify the IPv6 protocol for the ACL before you can configure the source and/or destination port.
Flow Label	Classifies IPv6 traffic based on a IPv6 Flow label field. This is a 20-bit field that is part of the IPv6 packet header. An IPv6 flow label can be used by a source station to label a set of packets belonging to the same flow. Select Any if all flow labels are acceptable or select User defined and then enter a specific flow label to be accepted by the ACL.

TCP Flags	Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. For each type of flag, select one of the following options: • Set—Match if the flag is SET. • Unset—Match if the flag is Not SET. • Don't care—Ignore the TCP flag.
Type of Service	The service type of the IP packet. • Any—Any service type • DSCP to match—Differentiated Serves Code Point (DSCP) to match. • IP Precedence to match—IP precedence is a model of TOS (type of service) that the network uses to help provide the appropriate QoS commitments. This model uses the 3 most significant bits of the service type byte in the IP header, as described in RFC 791 and RFC 1349.
ICMP	If the ACL is based on ICMP, select the ICMP message type that is used for filtering purposes. Either select the message type by name or enter the message type number. If all message types are accepted, select Any. • Any—All message types are accepted. • Select from list—Select message type by name from the drop-down list. • ICMP Type to Match—Number of message types that is to be used for filtering purposes.
ICMP Code	The ICMP messages may have a code field that indicates how to handle the message. Select one of the following options, to configure whether to filter on this code: • Any—Accept all codes. • User Defined—Enter an ICMP code for filtering purposes.

Step 5 Click **Apply**.

ACL Binding (VLAN)

When an ACL is bound to an interface, its ACE rules are applied to packets arriving at that interface. Packets that do not match any of the ACEs in the ACL are matched to a default rule, whose action is to drop unmatched packets. Although each interface can be bound to only one ACL, multiple interfaces can be bound to the same ACL by grouping them into a policy-map, and binding that policy-map to the interface. After an ACL is bound to an interface, it cannot be edited, modified, or deleted until it is removed from all the ports to which it is bound or in use.

Note It is possible to bind an interface (port, LAG or VLAN) to a policy or to an ACL, but they cannot be bound to both a policy and an ACL. In the same class map, a MAC ACL cannot be used with an IPv6 ACE that has a Destination IPv6 address as a filtering condition.

To bind an ACL to a VLAN, follow these steps:

Procedure

Step 1 Click **Access Control** > **ACL Binding (VLAN)**.

Step 2 Select a VLAN and click **Edit**.

If the VLAN you require is not displayed, add a new one.

Step 3 Select one of the following:

MAC-Based ACL	Select a MAC-based ACL to be bound to the interface.
IPv4-Based ACL	Select an IPv4-based ACL to be bound to the interface.
IPv6-Based ACL	Select an IPv6-based ACL to be bound to the interface.
Default Action	Select one of the following options: • Deny Any—If packet doesn't match an ACL, it's denied (dropped). • Permit Any—If packet doesn't match an ACL, it's permitted (forwarded). **Note** Default Action can be defined only if IP Source Guard isn't activated on the interface.

Step 4 Click **Apply**. The ACL binding is modified, and the Running Configuration file is updated.

Note If no ACL is selected, the ACL(s) that is previously bound to the VLAN are unbound.

ACL Binding (Port)

Access Control List (ACL) is a list of permissions applied on a port that filters the stream of packets transmitted to the port. A port can be bound with either a policy or an ACL, but not both. To bind an ACL to a port or LAG, follow these steps:

Procedure

Step 1 Click **Access Control** > **ACL Binding (Port)**.

Step 2 Select an interface type Ports/LAGs (Port or LAG).

Step 3 Click **Go**. For each type of interface selected, all interfaces of that type are displayed with a list of their current ACLs (for Input ACLs and Output ACLs):

Interface	Identifier of interface on which ACL is defined.
MAC ACL	ACLs of type MAC that are bound to the interface (if any).
IPv4 ACL	ACLs of type IPv4 that are bound to the interface (if any).
IPv6 ACL	ACLs of type IPv6 that are bound to the interface (if any).
Default Action	Action of the ACL's rules (drop any/permit any).

Step 4 To unbind all ACLs from an interface, select the interface, and click **Clear**.

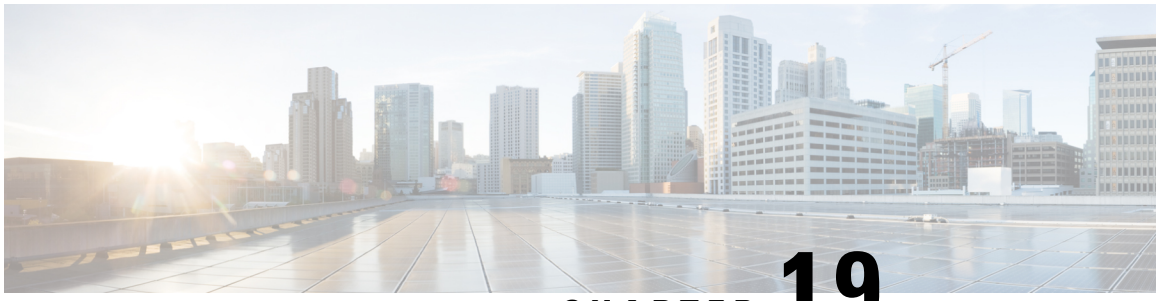
Step 5 Select an interface, and click **Edit**.

Step 6 Enter the following for both the Input ACL and Output ACL:

MAC-Based ACL	Select a MAC-based ACL to be bound to the interface.
IPv4-Based ACL	Select an IPv4-based ACL to be bound to the interface.
IPv6-Based ACL	Select an IPv6-based ACL to be bound to the interface.
Default Action	Select one of the following options: • Deny Any—If packet doesn't match an ACL, it's denied (dropped). • Permit Any—If packet doesn't match an ACL, it's permitted (forwarded). **Note** Default Action can be defined only if IP Source Guard isn't activated on the interface.

Step 7 Click **Apply**. The ACL binding is modified, and the Running Configuration file is updated.

Note
If no ACL is selected, the ACL(s) that is previously bound to the interface are unbound.



CHAPTER 19

Quality of Service

The Quality of Service feature is applied throughout the network to ensure that network traffic is prioritized according to required criteria and that the desired traffic receives preferential treatment. This chapter contains the following sections:

- General, on page 341
- QoS Basic Mode, on page 350
- QoS Advanced Mode, on page 352
- QoS Statistics, on page 360

General

Quality of Service (QoS) is a feature on the switch which prioritizes traffic resulting in a performance improvement for critical network traffic. QoS varies by switch, as the higher the level switch, the higher the network application layer it works with. The number of queues differ, as well as the kind of information used to prioritize.

QoS Properties

Quality of Service (QoS) prioritizes the traffic flow based on the type of traffic and can be applied to prioritize traffic for latency-sensitive applications (such as voice or video) and to control the impact of latency-insensitive traffic.

To configure QoS properties, follow these steps:

Procedure

Step 1 Click **Quality of Service** > **General** > **QoS Properties**.

Step 2 Set the QoS mode. The following options are available:

- Disable—QoS is disabled on the device.
- Basic—QoS is enabled on the device in Basic mode.
- Advanced—QoS is enabled on the device in Advanced mode.

Step 3 Select **Port/LAG** and click **GO** to display/modify all ports/LAGs on the device and their CoS information.

The following fields are displayed for all ports/LAGs:

- Interface—Type of interface.
- Default CoS—Default VPT value for incoming packets that do not have a VLAN Tag. The default CoS is 0.

Step 4 Click **Apply**. The Running Configuration file is updated.

To set QoS on an interface, select it, and click **Edit**.

Step 5 Enter the parameters.

- Interface—Select the port or LAG.
- Default CoS—Select the default CoS (Class-of-Service) value to be assigned for incoming packets (that do not have a VLAN tag).

Step 6 Click **Apply**. The interface default CoS value is saved to Running Configuration file.

To restore the default CoS values, click **Restore CoS Defaults**.

Queues

The device supports 8 queues for each interface. Queue number eight is the highest priority queue. Queue number one is the lowest priority queue.

There are two ways of determining how traffic in queues is handled, Strict Priority and Weighted Round Robin (WRR).

- Strict Priority—Egress traffic from the highest-priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, thus providing the highest level of priority of traffic to the highest numbered queue.
- Weighted Round Robin (WRR)—In WRR mode the number of packets sent from the queue is proportional to the weight of the queue (the higher the weight the more frames are sent). For example, if there are a maximum of four queues possible and all four queues are WRR and the default weights are used, queue 1 receives 1/15 of the bandwidth (assuming all queues are saturated and there's congestion), queue 2 receives 2/15, queue 3 receives 4/15 and queue 4 receives 8 /15 of the bandwidth. The type of WRR algorithm used in the device isn't the standard Deficit WRR (DWRR), but rather Shaped Deficit WRR (SDWRR).

The queuing modes can be selected in the Queue page. When the queuing mode is by strict priority, the priority sets the order in which queues are serviced, starting with the highest priority queue and going to the next lower queue when each queue is completed.

When the queuing mode is Weighted Round Robin, queues are serviced until their quota has been used up and then another queue is serviced. It's also possible to assign some of the lower queues to WRR, while keeping some of the higher queues in strict priority. In this case traffic for the strict-priority queues is always sent before traffic from the WRR queues. Only after the strict-priority queues have been emptied is traffic from the WRR queues forwarded. (The relative portion from each WRR queue depends on its weight).

To select the priority method and enter WRR data, complete the following steps:

Procedure

Step 1 Click **Quality of Service** > **General** > **Queue**.

Step 2 Enter the parameters.

- Queue—Displays the queue number.
- Scheduling Method—Select one of the following options:
  - Strict Priority—Traffic scheduling for the selected queue and all higher queues is based strictly on the queue priority.
  - WRR—Traffic scheduling for the selected queue is based on WRR. The period time is divided between the WRR queues that aren't empty, meaning they have descriptors to egress. This division happens only if the strict-priority queues are empty.
  - WRR Weight—If WRR is selected, enter the WRR weight assigned to the queue.
  - % of WRR Bandwidth—Displays the amount of bandwidth assigned to the queue. These values represent the percent of the WRR weight.

Step 3 Click **Apply**. The queues are configured, and the Running Configuration file is updated.

CoS/802.1p to a Queue

The CoS/802.1p to Queue page maps 802.1p priorities to egress queues. The CoS/802.1p to Queue Table determines the egress queues of the incoming packets based on the 802.1p priority in their VLAN Tags. For incoming untagged packets, the 802.1p priority is the default CoS/802.1p priority assigned to the ingress ports.

The following table describes the default mapping when there are 8 queues:

802.1p Values (0-7,7 being the highest)	Queue (8 queues 1-8,8 is the highest priority)	7 Queues	Notes
0	1	1	Background
1	2	1	Best Effort
2	3	2	Excellent Eff
3	6	5	Critical Appli SIP
4	5	4	Video
5	8	7	Voice - Cisco
6	8	7	Interwork Co
7	7	6	Network Con

By changing the CoS/802.1p to Queue mapping (CoS/802.1p to Queue) and the Queue schedule method and bandwidth allocation, it's possible to achieve the desired quality of service in a network.

The CoS/802.1p to Queue mapping is applicable only if one of the following exists:

- The device is in QoS Basic mode and CoS/802.1p trusted mode.
- The device is in QoS Advanced mode and the packets belong to flows that are CoS/802.1p trusted.

To map CoS values to egress queues, follow these steps:

Procedure

Step 1 Click **Quality of Service** > **General** > **CoS/802.1p to Queue**.

Step 2 Enter the parameters.

- 802.1p—Displays the 802.1p priority tag values to be assigned to an egress queue, where 0 is the lowest and 7 is the highest priority.
- Output Queue—Select the egress queue to which the 802.1p priority is mapped. Either four or eight egress queues are supported, where Queue 4 or Queue 8 is the highest priority egress queue and Queue 1 is the lowest priority.

Step 3 For each 802.1p priority, select the Output Queue to which it is mapped.

Step 4 Click **Apply, Cancel** or **Restore Defaults**. 801.1p priority values to queues are mapped, and the Running Configuration file is updated, the changes that entered are canceled, or previously defined values are restored.

DSCP to Queue

The DSCP (IP Differentiated Services Code Point) to Queue page maps DSCP values to egress queues. The DSCP to Queue Table determines the egress queues of the incoming IP packets based on their DSCP values. The original VPT (VLAN Priority Tag) of the packet is unchanged.

By simply changing the DSCP to Queue mapping and the Queue schedule method and bandwidth allocation, it's possible to achieve the desired quality of services in a network.

The DSCP to Queue mapping is applicable to IP packets if:

- The device is in QoS Basic mode and DSCP is the trusted mode.
- The device is in QoS Advanced mode and the packets belongs to flows that are DSCP trusted.

Non-IP packets are always classified to the best-effort queue.

The following tables describe the default DSCP to queue mapping for an 8-queue system where 7 is highest and 8 is used for stack control purposes.

DSCP	63	55	47	39	31	23	15	7
Queue	6	6	7	5	4	3	2	1
DSCP	62	54	46	38	30	22	14	6

Queue	6	6	7	5	4	3	2	1
DSCP	61	53	45	37	29	21	13	5
Queue	6	6	7	5	4	3	2	1
DSCP	60	52	44	36	28	20	12	4
Queue	6	6	7	5	4	3	2	1
DSCP	59	51	43	35	27	19	11	3
Queue	6	6	7	5	4	3	2	1
DSCP	58	50	42	34	26	18	10	2
Queue	6	6	7	5	4	3	2	1
DSCP	57	49	41	33	25	17	9	1
Queue	6	6	7	5	4	3	2	1
DSCP	56	48	40	32	24	16	8	0
Queue	6	6	6	7	6	6	1	1

The following tables describe the default DSCP to queue mapping for an 8-queue system where 8 is highest:

DSCP	63	55	47	39	31	23	15	7
Queue	7	7	8	6	5	4	3	1
DSCP	62	54	46	38	30	22	14	6
Queue	7	7	8	6	5	4	3	1
DSCP	61	53	45	37	29	21	13	5
Queue	7	7	8	6	5	4	3	1
DSCP	60	52	44	36	28	20	12	4
Queue	7	7	8	6	5	4	3	1
DSCP	59	51	43	35	27	19	11	3
Queue	7	7	8	6	5	4	3	1
DSCP	58	50	42	34	26	18	10	2
Queue	7	7	8	6	5	4	3	1
DSCP	57	49	41	33	25	17	9	1
Queue	7	7	8	6	5	4	3	1
DSCP	56	48	40	32	24	16	8	0

Queue	7	7	7	8	7	7	1	2

To map DSCP to queues, follow these steps:

Procedure

Step 1 Click **Quality of Service** > **General** > **DSCP to Queue**.

The DSCP to Queue page contains Ingress DSCP. It displays the DSCP value in the incoming packet and its associated class.

Step 2 Select the Output Queue (traffic forwarding queue) to which the DSCP value is mapped.

Step 3 Click **Apply**. The Running Configuration file is updated. Click **Restore Defaults** to restore the default settings.

Bandwidth

Note This setting is only available in the Advanced Setting view.

The Bandwidth page displays bandwidth information for each interface. To view the bandwidth information, complete the following steps:

Procedure

Step 1 Click **Quality of Service** > **General** > **Bandwidth**.

The fields in this page are described in the Edit page below, except for the following fields:

- **Ingress Rate Limit:**
  - Status—Displays whether Ingress Rate Limit is enabled.
  - Rate Limit (KBits/sec)—Displays the ingress rate limit for the port.
  - %—Displays the ingress rate limit for the port divided by the total port bandwidth.
  - CBS (Bytes)—Maximum burst size of data for the ingress interface in bytes of data
- **Egress Shaping Rates**:
  - Status—Displays whether Egress Shaping Rates is enabled.
  - CIR (KBits/sec)—Displays the maximum bandwidth for the egress interface.
  - CBS (Bytes)—Maximum burst size of data for the egress interface in bytes of data

Step 2 Select an interface, and click **Edit**.

Step 3 Select the Port or LAG interface.

Step 4 Enter the fields for the selected interface:

Option	Description
Ingress Rate Limit	Select to enable the ingress rate limit, which is defined in the field below. (Not relevant for LAGs).
Ingress Rate Limit (Kbits per sec)	Enter the maximum amount of bandwidth allowed on the interface. (Not relevant for LAGs).
Ingress Committed Burst Size (CBS)	Enter the maximum burst size of data for the ingress interface in bytes of data. This amount can be sent even if it temporarily increases the bandwidth beyond the allowed limit. This field is only available if the interface is a port. (Not relevant for LAGs).
Egress Shaping Rate	Select to enable egress shaping on the interface.
Committed Information Rate (CIR)	Enter the maximum bandwidth for the egress interface.
Egress Committed Burst Size (CBS)	Enter the maximum burst size of data for the egress interface in bytes of data. This amount can be sent even if it temporarily increases the bandwidth beyond the allowed limit.

Step 5 Click **Apply**. The bandwidth settings are written to the Running Configuration file.

Egress Shaping per Queue

This setting is only available in the Advanced Setting view.

In addition to limiting transmission rate per port, which is done in the Bandwidth page, the device can limit the transmission rate of selected egressing frames on a per-queue per-port basis. Egress rate limiting is performed by shaping the output load.

The device limits all frames except for management frames. Any frames that aren't limited are ignored in the rate calculations, meaning that their size isn't included in the limit total.

To configure the egress shaping per queue, complete the following steps:

Procedure

Step 1 Click **Quality of Service** > **General** > **Egress Shaping per Queue**.

The Egress Shaping Per Queue page displays the rate limit (CIR) and burst size (CBS) for each queue.

Step 2 Select an interface type (Port or LAG), and click **Go**.

Step 3 Select a Port/LAG, and click **Edit**.

This page enables shaping the egress for up to eight queues on each interface.

Step 4 Select the Interface.

Step 5 For each queue that is required, enter the following fields:

- Enable Shaping—Select to enable egress shaping on this queue.
- Committed Information Rate (CIR)—Enter the maximum rate (CIR) in Kbits per second (Kbps). CIR is the average maximum amount of data that can be sent.
- Committed Burst Size (CBS)—Enter the maximum burst size (CBS) in bytes. CBS is the maximum burst of data allowed to be sent even if a burst exceeds CIR.

Step 6 Click **Apply**. The bandwidth settings are written to the Running Configuration file.

VLAN Ingress Rate Limit

This setting is only available in the Advanced Setting view.

Rate limiting per VLAN, performed in the VLAN Ingress Rate Limit page, enables traffic limiting on VLANs. When VLAN ingress rate limiting is configured, it limits aggregate traffic from all the ports on the device.

The following constraints apply to rate limiting per VLAN:

- It has lower precedence than any other traffic policing defined in the system. For example, if a packet is subject to QoS rate limits but is also subject to VLAN rate limiting, and the rate limits conflict, the QoS rate limits take precedence.
- It's applied at the device level and within the device at the packet processor level. If there's more than one packet processor on the device, the configured VLAN rate limit value is applied to each of the packet processors, independently. Devices with up to 24 ports have a single packet processor, while devices of 48 ports or more have two packet processors.

Rate limiting is calculated separately for each packet processor in a unit.

To define the VLAN ingress rate limit, complete the following steps:

Procedure

Step 1 Click **Quality of Service** > **General** > **VLAN Ingress Rate Limit**.

This page displays the VLAN Ingress Rate Limit Table.

Step 2 Click **Add**.

Step 3 Enter the parameters.

- VLAN ID—Select a VLAN.
- Committed Information Rate (CIR)—Enter the average maximum amount of data that can be accepted into the VLAN in Kilobits per second.
- Committed Burst Size (CBS)—Enter the maximum burst size of data for the egress interface in bytes of data. This amount can be sent even if it temporarily increases the bandwidth beyond the allowed limit. Can't be entered for LAGs.

Step 4 Click **Apply**. The VLAN rate limit is added, and the Running Configuration file is updated.

iSCSI

This setting is only available in the Advanced Setting view.

This page enables activating iSCSI optimization, which means setting up a mechanism for giving priority to iSCSI traffic over other types of traffic. If this feature is enabled on a device, iSCSI traffic on any interface will be assigned the defined priority, and iSCSI traffic won't be subject to ACL or Policy rules set on interface.

iSCSI traffic is identified by the TCP port on which iSCSI targets listen to requests and optionally also by the IPv4 address on which iSCSI targets listen to requests. Two iSCSI IPv4 flows with well-known TCP ports 3260 and 860 are defined by default on device. iSCSI flow optimization is bi-directional, which means that it's applied to streams in both directions – from and to targets.

To enable and configure the mechanism for prioritizing and, optionally, marking iSCSI traffic, complete the following steps:

Procedure

Step 1 Click **Quality of Service** > **General** > **iSCSI**.

Step 2 Check **Enable** in the iSCSI Status field to enable processing iSCSI traffic on the device.

Step 3 Enter the fields under Quality of Service Settings:

- VPT Assignment—Select either Unchanged to leave the original VLAN Priority Tag (VPT) value in the packet or enter a new value in the Reassigned field.
- DSCP Assignment—Select either Unchanged to leave the original DSCP value in the packet or enter a value in the Reassigned field.
- Queue Assignment—Enter the Queue assignment for iSCSI traffic. By default it's assigned to Queue 7.

Step 4 Click **Apply** to save the settings.

The iSCSI Flow Table displays the various iSCSI flows that have been defined.Two iSCSI flows, with well-known TCP ports 3260 and 860, are displayed. The Flow Type of these flows is Default. If you add a new flow, its Flow Type is Static.

To add a new flow:

Step 5 Click **Add** and enter the following fields:

- TCP Port—This is the TCP port number on which the iSCSI target listens to requests. You can configure up to 8 target TCP ports on the switch.
- Target IP Address—Specifies the IP address of the iSCSI target (where data is stored). This is also the source of the iSCSI traffic. You can select **Any** to define a flow according to the TCP port parameter, or enter an IP address in User-Defined field to define a specific target address.

Step 6 Click **Apply** to save the settings.

Click **Restore Default Flows** to restore the default flows.

TCP Congestion Avoidance

This setting is only available in the Advanced Setting view.

The TCP Congestion Avoidance page enables activating a TCP congestion avoidance algorithm. The algorithm breaks up or avoids TCP global synchronization in a congested node, where the congestion is due to various sources sending packets with the same byte count.

To configure TCP congestion avoidance complete the following steps:

Procedure

Step 1 Click **Quality of Service** > **General** > **TCP Congestion Avoidance**.

Step 2 Click **Enable** to enable TCP congestion avoidance, and click **Apply**.

QoS Basic Mode

In QoS Basic mode, a specific domain in the network can be defined as trusted. Within that domain, packets are marked with 802.1p priority and/or DSCP to signal the type of service they require. Nodes within the domain use these fields to assign the packet to a specific output queue. The initial packet classification and marking of these fields is done in the ingress of the trusted domain.

QoS Global Settings

The Global Settings page contains information for enabling Trust on the device (see the Trust Mode field below). This configuration is active when the QoS mode is Basic mode. Packets entering a QoS domain are classified at the edge of the QoS domain.

To define the Trust configuration, complete the following steps:

Procedure

Step 1 Click **Quality of Service** > **QoS Basic Mode** > **Global Settings**.

Step 2 Select the Trust Mode while the device is either in Basic or Advanced mode. If a packet CoS level and DSCP tag are mapped to separate queues, the Trust mode determines the queue to which the packet is assigned:

- CoS/802.1p—Traffic is mapped to queues based on the VPT field in the VLAN tag, or based on the per-port default CoS/802.1p value (if there's no VLAN tag on the incoming packet), the actual mapping of the VPT to queue can be configured in the mapping CoS/802.1p to Queue page.

- DSCP—All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured in the DSCP to Queue page. If traffic isn't IP traffic, it's mapped to the best effort queue.
- CoS/802.1p-DSCP—Either CoS/802.1p or DSCP whichever has been set.

Step 3 Select **Override Ingress DSCP** to override the original DSCP values in the incoming packets with the new values entered in the DSCP Override table. When Override Ingress DSCP is enabled, the device uses the new DSCP values for egress queuing. It also replaces the original DSCP values in the packets with the new DSCP values.

Note
The frame is mapped to an egress queue using the new, rewritten value, and not by the original DSCP value.

Step 4 Click **DSCP Override Table** to reconfigure DSCP. (See DSCP Override Table).

Step 5 DSCP In displays the DSCP value of the incoming packet that needs to be re-marked to an alternative value. Select the DSCP Out value to indicate the outgoing value is mapped.

Step 6 Click **Apply**. The Running Configuration file is updated with the new DSCP values. Click **Restore Defaults** to go back to the default settings.

QoS Interface Settings

The Interface Settings page enables configuring QoS on each port of the device, as follows:

- QoS State Disabled on an Interface—All inbound traffic on the port is mapped to the best effort queue and no classification/prioritization takes place.
- QoS State of the Port is Enabled—Port prioritize traffic on ingress is based on the system-wide configured trusted mode, which is either CoS/802.1p trusted mode or DSCP trusted mode.

To enter QoS settings per interface, complete the following steps:

Procedure

Step 1 Click **Quality of Service** > **QoS Basic Mode** > **Interface Settings**.

Step 2 Use the filter to select the Interface Type (Port or Lag) and click **Go** to display the current settings. QoS State displays whether QoS is enabled on the interface

Step 3 Select an interface, and click **Edit**.

Step 4 Select the Port or LAG interface.

Step 5 Click to enable or disable QoS State for this interface.

Step 6 Click **Apply**. The Running Configuration file is updated.

QoS Advanced Mode

Frames that match an ACL and permitted entrance are implicitly labeled with the name of the ACL that permitted their entrance. Advanced mode QoS actions can then be applied to these flows.

In QoS advanced mode, the device uses policies to support per flow QoS. A policy and its components have the following characteristics and relationships:

- A policy contains one or more class maps.
- A class map defines a flow with one or more associating ACLs. Packets that match only ACL rules (ACE) in a class map with Permit (forward) action are considered belonging to the same flow, and are subjected to the same quality of services. Thus, a policy contains one or more flows, each with a user defined QoS.
- The QoS of a class map (flow) is enforced by the associating policer. There are two type of policers, single policer and aggregate policer. Each policer is configured with a QoS specification. A single policer applies the QoS to a single class map, and thus to a single flow, based on the policer QoS specification. An aggregate policer applies the QoS to one or more class maps, and thus one or more flows. An aggregate policer can support class maps from different policies.

  The 2 Rate 3 Color (2R3C) feature is supported on the device. In this feature, every policer has two thresholds. If the first threshold is reached, a user-configured Exceed action is performed. If the second threshold is reached, a user-configured Violate action is performed.
- Per flow QoS are applied to flows by binding the policies to the desired ports. A policy and its class maps can be bound to one or more ports, but each port is bound with at most one policy.

Global Settings

The Global Settings page contains information for enabling Trust on the device. Packets entering a QoS domain are classified at the edge of the QoS domain.

To define the Trust configuration:

Procedure

Step 1 Click **Quality of Service** > **QoS Advanced Mode** > **Global Settings**.

Step 2 Select the Trust Mode while the device is in Advanced mode. If a packet CoS level and DSCP tag are mapped to separate queues, the Trust mode determines the queue to which the packet is assigned:

- CoS/802.1p—Traffic is mapped to queues based on the VPT field in the VLAN tag, or based on the per-port default CoS/802.1p value (if there's no VLAN tag on the incoming packet), the actual mapping of the VPT to queue can be configured in the mapping CoS/802.1p to Queue page.
- DSCP—All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured in the DSCP to Queue page. If traffic isn't IP traffic, it's mapped to the best effort queue.
- CoS/802.1p-DSCP—Select to use Trust CoS mode for non-IP traffic and Trust DSCP for IP traffic.

Step 3 Select the default Advanced mode QoS trust mode (either trusted or untrusted) for interfaces in the Default Mode Status field. This provides basic QoS functionality on Advanced QoS, so that you can trust CoS/DSCP on Advanced QoS by default (without having to create a policy).

Step 4 In QoS Advanced Mode, when the Default Mode Status is set to Not Trusted, the default CoS values configured on the interface is ignored and all the traffic goes to queue 1. See the Quality of Service > QoS Advanced Mode > Global Settings page for details.

Step 5 If you have a policy on an interface then the Default Mode is irrelevant, the action is according to the policy configuration and unmatched traffic is dropped.

Step 6 Select **Override Ingress DSCP** to override the original DSCP values in the incoming packets with the new values according to the DSCP Override Table. When Override Ingress DSCP is enabled, the device uses the new DSCP values for egress queuing. It also replaces the original DSCP values in the packets with the new DSCP values.

Note
The frame is mapped to an egress queue using the new, rewritten value, and not by the original DSCP value.

Step 7 If Override Ingress DSCP was enabled, click **DSCP Override Table** to reconfigure DSCP.

a) In The DSCP Override Table, enter the following fields:

- DSCP In—Displays the DSCP value of the incoming packet that needs to be remarked to an alternative value.
- DSCP Out—Select the DSCP Out value to indicate the outgoing value is mapped.

b) Click **Apply**. To go back to the default settings, click **Restore Defaults**.

Out-of-Profile DSCP Remarking

When a policer is assigned to a class maps (flows), you can specify the action to take when the amount of traffic in one or more flows exceeds the QoS-specified limits. The portion of the traffic that causes the flow to exceed its QoS limit is referred to as out-of-profile packets. If the exceed/violate action is Out of Profile DSCP, the device remaps the original DSCP value of the out-of-profile IP packets with a new value based on the Out of Profile DSCP Remarking Table. The device uses the new values to assign resources and the egress queues to these packets. The device also physically replaces the original DSCP value in the out of profile packets with the new DSCP value.

To use the out-of-profile DSCP exceed action, remap the DSCP value in the Out Of Profile DSCP Remarking Table. Otherwise the action is null, because the DSCP value in the table remaps the packets to itself by factory default. This feature changes the DSCP tags for incoming traffic switched between trusted QoS domains. Changing the DSCP values used in one domain, sets the priority of that type of traffic to the DSCP value used in the other domain to identify the same type of traffic. These settings are active when the system is in the QoS Advance mode, and once activated they are active globally. This can be configured in the QoS Properties, on page 341.

To map DSCP values, follow these steps:

Procedure

Step 1 Click **Quality of Service** > **QoS Advanced Mode** > **Out of Profile DSCP Remarking**. This page enables setting the DSCP-value of traffic entering or leaving the device.

DSCP In displays the DSCP value of the incoming packet that needs to be re-marked to an alternative value.

Step 2 Select the DSCP Out value to where the incoming value is mapped.

Step 3 Click **Apply**. The Running Configuration file is updated with the new DSCP Remarking table.

Step 4 Click **Restore Defaults** to restore the factory CoS default setting for this interface.

Class Mapping

A Class Map defines a traffic flow with ACLs (Access Control Lists) defined on it. A MAC ACL, IP ACL, and IPv6 ACL can be combined into a class map. Class maps are configured to match packet criteria on a match-all or match-any basis. They are matched to packets on a first-fit basis, meaning that the action associated with the first-matched class map is the action performed by the system. Packets that match the same class map are considered to belong to the same flow.

Note Defining class maps doesn't have any effect on QoS; it's an interim step, enabling the class maps to be used later.

If more complex sets of rules are needed, several class maps can be grouped into a supergroup called a policy.

In the same class map, a MAC ACL can't be used with an IPv6 ACE that has a Destination IPv6 address as a filtering condition.

The Class Mapping page shows the list of defined class maps and the ACLs comprising each, and enables you to add/delete class maps.

To define a Class Map, complete the following steps:

Procedure

Step 1 Click **Quality of Service** > **QoS Advanced Mode** > **Class Mapping**.

For each class map, the ACLs defined on it are displayed along with the relationship between them. Up to three ACLs can be displayed along with their Match, which can be either And or Or. This indicates the relationship between the ACLs. The Class Map is then the result of the three ACLs combined with either And or Or.

Step 2 Click **Add**.

A new class map is added by selecting one or two ACLs and giving the class map a name. If a class map has two ACLs, you can specify that a frame must match both ACLs, or that it must match either one or both of the ACLs selected.

Step 3 Enter the parameters.

- Class Map Name—Enter the name of a new class map.
- Match ACL Type—The criteria that a packet must match in order to be considered to belong to the flow defined in the class map. The options are:
  - IP—A packet must match either of the IP-based ACLs in the class map.
  - MAC—A packet must match the MAC-based ACL in the class map.

- IP and MAC—A packet must match the IP-based ACL and the MAC-based ACL in the class map.
- IP or MAC—A packet must match either the IP-based ACL or the MAC-based ACL in the class map.

- IP—Select the IPv4 based ACL or the IPv6 based ACL for the class map.
- MAC—Select the MAC-based ACL for the class map.
- Preferred ACL—Select whether packets are first matched to an IP or MAC.

Step 4 Click **Apply**. The Running Configuration file is updated.

Aggregate Policer

You can measure the rate of traffic that matches a predefined set of rules. To enforce limits, use ACLs in one or more class maps to match the desired traffic, and use a policer to apply the QoS on the matching traffic.

A policer is configured with a QoS specification. There are two kinds of policers:

- Single (Regular) Policer—A single policer applies the QoS to a single class map, and to a single flow based on the policer's QoS specification. When a class map using single policer is bound to multiple ports, each port has its own instance of single policer. Thus, each applying the QoS on the class map (flow) at ports that are otherwise independent of each other. A single policer is created in the Policy Table page.
- Aggregate Policer—An aggregate policer applies the QoS to one or more class maps, and one or more flows. An aggregation policer can support class maps from different policies. An aggregate policer applies QoS to all its flows in aggregation regardless of policies and ports. An aggregate policer is created in the Aggregate Policer page.

  An aggregate policer is defined if the policer is to be shared with more than one class. Policers on a port can’t be shared with other policers in another device.

Each policer is defined with its own QoS specification with a combination of the following parameters:

- Peak Enforcement—Select to enable action if peak burst size is exceeded.
- Peak Information Rate (PIR)—Enter the peak traffic rate (PIR) in kbits per second (kbps).
- Peak Burst Size (PBS)—Enter the peak burst size (PBS) in bytes.
- Violate Action—Select one of the following actions if peak size is exceeded:
  - Drop—Drop the frames violating the peak size.
  - Out-of-Profile DSCP—Mark frames violating the peak size with the DSCP value with previously set DSCP value
- A maximum allowed rate, called a Committed Information Rate (CIR), measured in Kbps.
- An amount of traffic, measured in bytes, called a Committed Burst Size (CBS). This is traffic that is allowed to pass as a temporary burst even if it’s above the defined maximum rate.

- An action to be applied to frames that are over the limits (called out-of-profile traffic), where such frames can be passed as is, dropped, or passed, but remapped to a new DSCP value that marks them as lower-priority frames for all subsequent handling within the device.
- Configures traffic policing on the basis of the specified rates and optional actions Enter the CIR and these optional values and actions

Assigning a policer to a class map is done when a class map is added to a policy. If the policer is an aggregate policer, you must create it using the Aggregate Policer page.

To define an aggregate policer, complete the following steps:

Procedure

Step 1 Click **Quality of Service** > **QoS Advanced Mode** > **Aggregate Policer**.

This page displays the existing aggregate policers.

Step 2 Click **Add**.

Step 3 Enter the parameters.

- Aggregate Policer Name—Enter the name of the Aggregate Policer.
- Ingress Committed Information Rate (CIR)—Enter the maximum bandwidth allowed in bits per second. See the description of this in the Bandwidth, on page 346.
- Ingress Committed Burst Size (CBS)—Enter the maximum burst size (even if it goes beyond the CIR) in bytes. See the description of this in the Bandwidth, on page 346.
- Exceed Action—Select the action to be performed on incoming packets that exceed the CIR. Possible values are:
  - Drop—Packets exceeding the defined CIR value are dropped.
  - Out of Profile DSCP—The DSCP values of packets exceeding the defined CIR value are remapped to a value based on the Out Of Profile DSCP Remarking Table.
- Peak Enforcement—Select to enable action if peak burst size is exceeded.
- Peak Information Rate (PIR)—Enter the peak traffic rate (PIR) in kbits per second (kbps).
- Peak Burst Size (PBS)—Enter the peak burst size (PIR) in bytes.
- Violate Action—Select one of the following actions if peak size is exceeded:
  - Drop—Drop the frames violating the peak size.
  - Out-of-Profile DSCP—Mark frames violating the peak size with the DSCP value with previously set DSCP value

Step 4 Click **Apply**. The Running Configuration file is updated.

Policy Table

The Policy Table Map page displays the list of advanced QoS policies defined in the system. The page also allows you to create and delete policies. Only those policies that are bound to an interface are active (see Policy Binding, on page 359).

Each policy consists of:

- One or more class maps of ACLs which define the traffic flows in the policy.
- One or more aggregates that applies the QoS to the traffic flows in the policy.

After a policy has been added, class maps can be added by using the Policy Table page. To add a QoS policy, complete the following steps:

Procedure

Step 1 Click **Quality of Service** > **QoS Advanced Mode** > **Policy Table**.

This page displays the list of defined policies.

Step 2 Click **Policy Class Map Table** to display the Policy Class Maps page or click **Add** to open the Add Policy Table page.

Step 3 Enter the name of the new policy in the New Policy Name field.

Step 4 Click **Apply**. The QoS policy profile is added, and the Running Configuration file is updated.

Policy Class Maps

One or more class maps can be added to a policy. A class map defines the type of packets that are considered to belong to the same traffic flow.

To add a class map to a policy:

Procedure

Step 1 Click **Quality of Service** > **QoS Advanced Mode** > **Policy Class Maps**.

Step 2 Select a policy in the Filter, and click **Go**. All class maps in that policy are displayed.

Step 3 To add a new class map, click **Add**.

Step 4 Enter the following parameters.

Policy Name	Displays the policy to which the class map is being added.
Class Map Name	Select an existing class map to be associated with the policy. Class maps are created in the Class Mapping page.

Action Type	Select the action regarding the ingress CoS/802.1p and/or DSCP value of all the matching packets. • Use default trust mode—If this option is selected, use the default mode status in Global Trust mode. If the default mode status is "Not Trusted", ignore the ingress CoS/802.1p and/or DSCP value and the matching packets are sent as best effort. • Always Trust—If this option is selected, the device trusts the matching packet based on the Global Trust mode (selected in the Global Settings page). It ignores the Default Mode status (selected in the Global Settings page). • Set—If this option is selected, use the value entered in the New Value box to determine the egress queue of the matching packets as follows: If the new value (0..7) is a CoS/802.1p priority, use the priority value and the CoS/802.1p to Queue Table to determine the egress queue of all the matching packets. If the new value (0..63) is a DSCP, use the new DSCP and the DSCP to Queue Table to determine the egress queue of the matching IP packets. Otherwise, use the new value (1..8) as the egress queue number for all the matching packets.
Traffic Redirect	Select whether to redirect matching traffic. If so, select the unit/port to which traffic will be redirected.
Traffic Mirror	Set to mirror a traffic flow to an analyzer Ethernet port. If this option is selected the traffic is mirrored to the destination port specified in SPAN Session ID 1. If no target port is specified in SPAN session ID 1 the mirror action won't have effect. If a policy class map with Traffic Mirror action is applied to an interface – and that same interface is defined as a source port for SPAN session 1 – all traffic, and not only specific flow, will be mirrored. Additional rules and actions of the policy (and ACL) applied to the interface are still enforced even when Traffic Mirror action is configured. For example: • If the ACL action of the mirrored flow is permitted – in addition to being mirrored – the flow traffic is also be forwarded. If the action of flow ACL is deny – flow traffic will be mirrored but not forwarded to the egress network interface (drop behavior). • Traffic flows on interfaces, to which policy is applied that don't match the Mirrored class map classification, follow the default policy default action.
Police Type	Select the policer type for the policy. The options are: • None—No policy is used. • Single—The policer for the policy is a single policer. • Aggregate—The policer for the policy is an aggregate policer.

Step 5 If Police Type is Aggregate, select the Aggregate Policer.

Step 6 If Police Type is Single, enter the following QoS parameters:

Ingress Committed Information Rate (CIR)	Enter the CIR in Kbps. See a description of this in the Bandwidth page.

Ingress Committed Burst Size (CBS)	Enter the CBS in bytes. See a description of this in the Bandwidth page.
Exceed Action	Select the action assigned to incoming packets exceeding the CIR. The options are: • Drop—Packets exceeding the defined CIR value are dropped. • Out of Profile DSCP—IP packets exceeding the defined CIR are forwarding with a new DSCP derived from the Out Of Profile DSCP Remarking Table.
Peak Enforcement	Select to enable action if peak burst size is exceeded.
Peak Information Rate (PIR)	Enter the peak traffic rate (PIR) in kbits per second (kbps).
Peak Burst Size (PBS)	Enter the peak burst size (PIR) in kbits per second (kbps).
Violate Action	Select one of the following actions if peak size is exceeded. • Drop—Drop the frames violating the peak size. • Out of Profile DSCP—Mark frames violating the peak size with the DSCP value with previously set DSCP value

Step 7 Click **Apply**.

Policy Binding

The Policy Binding page shows which policy profile is bound and to which port. A policy can be bound to an interface as an ingress (input) policy or as an egress (output) policy. When a policy profile is bound to a specific port, it's active on that port. Only one policy profile can be configured per port and per direction. However, a single policy can be bound to more than one port.

When a policy is bound to a port, it filters and applies QoS to traffic that belongs to the flows defined in the policy.

To edit a policy, it must first be removed (unbound) from all those ports to which it's bound.

Note It's possible to either bind a port to a policy or to an ACL but both can't be bound.

To define policy binding, complete the following steps:

Procedure

Step 1 Click **Quality of Service** > **QoS Advanced Mode** > **Policy Binding**.

Step 2 Select an Interface Type if required.

Step 3 Click **Go**. The policies for that interface are displayed.

Step 4 Click **Edit**.

Step 5 Select the following for the input policy/interface:

- Input Policy Binding—Select to bind the input policy to the interface.
- Policy Name—Select the input policy being bound.
- Default Action—Select action if packet matches policy:
  - Deny Any—Select to forward packets on the interface if they match any policy.
  - Permit Any—Select to forward packets on the interface if they don't match any policy.

Note
Permit Any can be defined only if IP Source Guard isn't activated on the interface.

Step 6 Select the following for the output policy/interface:

- Output Policy Binding—Select to bind the output policy to the interface.
- Policy Name—Select the output policy being bound.
- Default Action—Select action if packet matches policy:
  - Deny Any—Select to forward packets on the interface if they match any policy.
  - Permit Any—Select to forward packets on the interface if they don't match any policy.

Note
Permit Any can be defined only if IP Source Guard isn't activated on the interface.

Step 7 Click **Apply**. The QoS policy binding is defined, and the Running Configuration file is updated.

QoS Statistics

QoS statistics feature allows you to gather statistics for the rate at which packets are forwarded out of a queue and for the rate at which committed, conformed, or exceeded packets are dropped on the device.

Single Policer Statistics

The Single Policer Statistics page indicates the number of in-profile and out-of-profile packets that are received from an interface that meet the conditions defined in the class map of a policy.

Note This page isn't displayed when the device is in Layer 3 mode.

To view policer statistics:

Procedure

Step 1 Click **Quality of Service** > **QoS Statistics** > **Single Policer Statistics**.

This page displays the following fields:

- Interface—Statistics are displayed for this interface.
- Policy—Statistics are displayed for this policy.
- Class Map—Statistics are displayed for this class map.
- In-Profile Bytes—Number of in-profile bytes received.
- Out-of-Profile Bytes—Number of outprofile bytes received.

Step 2 Click **Add.**

Step 3 Enter the parameters.

- Interface—Select the interface for which statistics are accumulated.
- Policy Name—Select the policy name.
- Class Map Name—Select the class name.

Step 4 Click **Apply**. An additional request for statistics is created and the Running Configuration file is updated.

Aggregate Policer Statistics

To view aggregated policer statistics:

Procedure

Step 1 Click **Quality of Service** > **QoS Statistics** > **Aggregate Policer Statistics**.

This page displays the following fields:

- Aggregate Policer Name—Policer on which statistics are based.
- In-Profile Bytes—Number of in-profile packets that received.
- Out-of-Profile Bytes—Number of out-of-profile packets that received.

Step 2 Click **Add**.

Step 3 Select an Aggregate Policer Name, one of the previously-created Aggregate Policers for which statistics are displayed.

Step 4 Click **Apply**. An additional request for statistics is created, and the Running Configuration file is updated.

Step 5 Click **Delete** to remove a specific statistic.

Step 6 Click **Clear Counters** to clear the counters of the selected policer.

Queue Statistics

The Queues Statistics page displays queue statistics, including statistics of forwarded and dropped packets, based on interface, queue, and drop precedence.

To view Queues Statistics and define what statistics to display (Counter Set):

Procedure

Step 1 Click **Quality of Service** > **QoS Statistics** > **Queue Statistics**.

This page displays the following fields:

- Refresh Rate—Select the time period that passes before the interface Ethernet statistics are refreshed. The available options are:
  - No Refresh—Statistics aren't refreshed.
  - 15 Sec—Statistics are refreshed every 15 seconds.
  - 30 Sec—Statistics are refreshed every 30 seconds.
  - 60 Sec—Statistics are refreshed every 60 seconds.

To view a specific unit and interface, select the unit/interface in the filter and click **Go**.

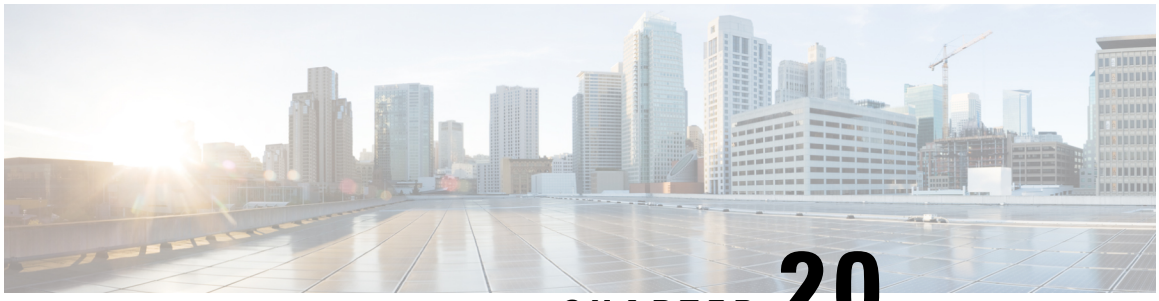
To view a specific interface, select the interface in the filter and click **Go**.

The Queue Statistics Table displays the following fields for each queue:

- Queue—Packets forwarded or tail dropped from this queue.
- Transmitted Packets—Number of packets that were transmitted.
- Tail Dropped Packets—Number of packets that were tail dropped.
- Transmitted Bytes—Number of bytes that were transmitted.
- Tail Dropped Bytes—Number of bytes that were tail dropped.

Step 2 Click **Clear Interface Counters** to clear the statistic counters for the selected interface.

Step 3 Click **Clear All Interface Counters** to clear the statistic counters for all interfaces.



CHAPTER 20

SNMP

This chapter describes the Simple Network Management Protocol (SNMP) feature that provides a method for managing network devices. It contains the following sections:

- Engine ID, on page 363
- SNMP Views, on page 365
- SNMP Groups, on page 366
- SNMP Users, on page 367
- SNMP Communities, on page 369
- Trap Settings, on page 370
- Notification Recipients SNMPv1,2, on page 371
- Notification Recipients SNMPv3, on page 372
- Notification Filter, on page 374

Engine ID

The Engine ID is used by SNMPv3 entities to uniquely identify them. An SNMP agent is considered an authoritative SNMP engine. This means that the agent responds to incoming messages (Get, GetNext, GetBulk, Set) and sends trap messages to a manager. The agent's local information is encapsulated in fields in the message.

Each SNMP agent maintains local information that is used in SNMPv3 message exchanges. The default SNMP Engine ID is comprised of the enterprise number and the default MAC address. This engine ID must be unique for the administrative domain, so that no two devices in a network have the same engine ID.

Local information is stored in four MIB variables that are read-only (snmpEngineId, snmpEngineBoots, snmpEngineTime, and snmpEngineMaxMessageSize).

⚠

Caution When the engine ID is changed, all configured users and groups are erased.

To configure the SNMP engine ID, complete the following steps:

Procedure

Step 1 Click **SNMP** > **Engine ID**.

Step 2 Choose which to use for Local Engine ID.

- Use Default—Select to use the device-generated engine ID. The default engine ID is based on the device MAC address, and is defined per standard as:
  - First 4 octets—First bit = 1, the rest is the IANA enterprise number.
  - Fifth octet—Set to 3 to indicate the MAC address that follows.
  - Last 6 octets—MAC address of the device
- None—No engine ID is used.
- User Defined—Enter the local device engine ID. The field value is a hexadecimal string (range: 10–64). Each byte in the hexadecimal character strings is represented by two hexadecimal digits.

  All remote engine IDs and their IP addresses are displayed in the Remote Engine ID table.

Step 3 Click **Apply**. The Running Configuration file is updated.

The Remote Engine ID table shows the mapping between IP addresses of the engine and Engine ID.

To add the IP address of an engine ID:

Step 4 Click **Add**. Enter the following fields:

- Server Definition—Select whether to specify the Engine ID server by IP address or name.
- IP Version—Select the supported IP format.
- IPv6 Address Type—Select the IPv6 address type (if IPv6 is used). The options are:
  - Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication on the local network only. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- Link Local Interface—Select the link local interface (if IPv6 Address Type Link Local is selected) from the list.
- Server IP Address/Name—Enter the IP address or domain name of the log server.
- Engine ID—Enter the Engine ID.

Step 5 Click **Apply**. The Running Configuration file is updated.

SNMP Views

A view is a user-defined label for a collection of MIB subtrees. Each subtree ID is defined by the Object ID (OID) of the root of the relevant subtrees. Either well-known names can be used to specify the root of the desired subtree or an OID can be entered. The Views page enables creating and editing SNMP views. The default views (Default, DefaultSuper) can't be changed.

Views can be attached to groups or to a community which employs basic access mode through the SNMP Groups, on page 366.

To configure the SNMP views, complete the following steps:

Procedure

Step 1 Click **SNMP** > **Views**.

The following fields are displayed for each view:

- Object ID Subtree—Node in the MIB tree that is included or excluded in the view.
- Object ID Subtree View—Whether the node is Included or Excluded.

Step 2 Click **Add** to define new views.

Step 3 Enter the parameters.

- View Name—Enter a view name 0–30 characters.
- Object ID Subtree—Select the node in the MIB tree that is included or excluded in the selected SNMP view. The options to select the object are as follows:
  - Select from list—Enables you to navigate the MIB tree.
  - User Defined—Enter an OID not offered in the Select from list option.

Step 4 Select or deselect **Include in view.** If this is selected, the selected MIBs are included in the view, otherwise they are excluded.

Step 5 Click **Apply**.

Step 6 In order to verify your view configuration, select the user-defined views from the Filter: View Name list.

- Default—Default SNMP view for read and read/write views.
- DefaultSuper—Default SNMP view for administrator views.

SNMP Groups

In SNMPv1 and SNMPv2, a community string is sent along with the SNMP frames. The community string acts as a password to gain access to an SNMP agent. However, neither the frames nor the community string is encrypted. Therefore, SNMPv1 and SNMPv2 aren't secure.

In SNMPv3, the following security mechanisms can be configured.

- Authentication—The device checks that the SNMP user is an authorized system administrator. This is done for each frame.
- Privacy—SNMP frames can carry encrypted data.

Thus, in SNMPv3, there are three levels of security:

- No security (No authentication and no privacy)
- Authentication (Authentication and no privacy)
- Authentication and privacy

SNMPv3 provides a means of controlling the content each user can read or write and the notifications they receive. A group defines read/write privileges and a level of security. It becomes operational when it's associated with an SNMP user or community.

Note To associate a non-default view with a group, first create the view in the SNMP Views, on page 365.

To create an SNMP group, complete the following steps:

Procedure

Step 1 Click **SNMP** > **Groups**.

This page contains the existing SNMP groups and their security levels.

Step 2 Click **Add**.

Step 3 Enter the parameters.

- Group Name—Enter a new group name.
- Security Model—Select the SNMP version attached to the group, SNMPv1, v2, or v3.

  Three types of views with various security levels can be defined. For each security level, select the views for Read, Write, and Notify by entering the following fields:
- Enable—Select this field to enable the Security Level.
- Security Level—Define the security level attached to the group. SNMPv1 and SNMPv2 support neither authentication nor privacy. If SNMPv3 is selected, choose one of the following:
  - No Authentication and No Privacy—Neither the Authentication nor the Privacy security levels are assigned to the group.

- Authentication and No Privacy—Authenticates SNMP messages, and ensures that the SNMP message origin is authenticated but doesn't encrypt them.
- Authentication and Privacy—Authenticates SNMP messages, and encrypts them.

- View—Select to associate a view with either read, write, and/or notify access privileges of the group limits the scope of the MIB tree to which the group has read, write, and notify access.
  - Read—Management access is read-only for the selected view. Otherwise, a user or a community associated with this group is able to read all MIBs except those that control SNMP itself.
  - Write—Management access is written for the selected view. Otherwise, a user or a community associated with this group is able to write all MIBs except those that control SNMP itself.
  - Notify—Limits the available content of the traps to those included in the selected view. Otherwise, there's no restriction on the contents of the traps. This can only be selected for SNMPv3.

Step 4 Click **Apply**. The SNMP group is saved to the Running Configuration file.

SNMP Users

An SNMP user is defined by the login credentials (username, passwords, and authentication method) and by the context and scope in which it operates by association with a group and an Engine ID. The configured users have the attributes of its group, having the access privileges configured within the associated view.

To create an SNMPv3 user, the following must first exist:

- An engine ID must first be configured on the device. This is done in the Engine ID, on page 363.
- An SNMPv3 group must be available. An SNMPv3 group is defined in the SNMP Groups, on page 366.

To display SNMP users and define new ones:

Procedure

Step 1 Click **SNMP** > **Users**.

This page displays existing users. The fields in this page are described in the Add page except for the following field:

- IP Address—Displays the IP address of the engine.

Step 2 Click **Add.**

This page provides information for assigning SNMP access control privileges to SNMP users.

Step 3 Enter the parameters.

- User Name—Enter a name for the user.

- Engine ID—Select either the local or remote SNMP entity to which the user is connected. Changing or removing the local SNMP Engine ID deletes the SNMPv3 User Database. To receive inform messages and request information, you must define both a local and remote user.
  - Local—User is connected to the local device.
  - Remote IP Address—User is connected to a different SNMP entity in addition to the local device. If the remote Engine ID is defined, remote devices receive inform messages, but can't make requests for information.
- Group Name—Select the SNMP group to which the SNMP user belongs. SNMP groups are defined in the Add Group page.

  Note
  Users, who belong to groups which have been deleted, remain, but they are inactive.

- Authentication Method—Select the Authentication method that varies according to the Group Name assigned. If the group doesn't require authentication, then the user can't configure any authentication. The options are:
  - None—No user authentication is used.
  - SHA—A password that is used for generating a key by the SHA-1 (Secure Hash Algorithm) authentication method.
  - SHA224- A password that is used for generating a key by the SHA-224 (based on Secure Hash Algorithm 2) authentication method truncated to 128 bits.
  - SHA256- A password that is used for generating a key by the SHA-256 (based on Secure Hash Algorithm 2) authentication method truncated to 192 bits.
  - SHA384- A password that is used for generating a key by the SHA-384 (based on Secure Hash Algorithm 2) authentication method truncated to 256 bits.
  - SHA512- A password that is used for generating a key by the SHA-512 (based on Secure Hash Algorithm 2) authentication method truncated to 384 bits.
- Authentication Password—If authentication is accomplished by password and authentication method, enter the local user password in either Encrypted or Plaintext. Local user passwords are compared to the local database. And can contain up to 32 ASCII characters.
- Privacy Method—Select one of the following options:
  - None—Privacy password isn't encrypted.
  - AES—Privacy password is encrypted according to the AES.
- Privacy Password—16 bytes are required (AES encryption key) if the AES privacy method was selected. This field must be exactly 32 hexadecimal characters. The Encrypted or Plaintext mode can be selected.

Step 4 Click **Apply** to save the settings.

SNMP Communities

Access rights in SNMPv1 and SNMPv2 are managed by defining communities in the Communities page. The community name is a type of shared password between the SNMP management station and the device. It's used to authenticate the SNMP management station.

Communities are only defined in SNMPv1 and v2 because SNMPv3 works with users instead of communities. The users belong to groups that have access rights assigned to them. The Communities page associates communities with access rights, either directly (Basic mode) or through groups (Advanced mode):

- Basic mode—The access rights of a community can configure with Read Only, Read Write, or SNMP Admin. In addition, you can restrict the access to the community to only certain MIB objects by selecting a view (defined in the SNMP Users, on page 367).
- Advanced Mode—The access rights of a community are defined by a group (defined in the SNMP Groups, on page 366). You can configure the group with a specific security model. The access rights of a group are Read, Write, and Notify.

To define the SNMP communities, complete the following steps:

Procedure

Step 1 Click **SNMP** > **Communities**.

Step 2 Click **Add** to define and configure new SNMP community.

Step 3 Configure the following fields:

SNMP Management Station	Select one of the following options: • All—to indicate that any IP device can access the SNMP community. • User Defined—to enter the management station IP address that can access the SNMP community.
IP Version	Select either IPv4 or IPv6.
IPv6 Address Type	Select the supported IPv6 address type if IPv6 is used. The options are: • Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication on the local network only. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration. • Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
Link Local Interface	If the IPv6 address type is Link Local, select whether it's received through a VLAN or ISATAP.
IP Address	Enter the SNMP management station IP address.

Community String	Enter the community name used to authenticate the management station to the device.
Basic	In this community type, there's no connection to any group. You can only choose the community access level (Read Only, Read Write, or SNMP Admin) and, optionally, further qualify it for a specific view. By default, it applies to the entire MIB. If this is selected, enter the following fields: • Access Mode—Select the access rights of the community. The options are: Read Only—Management access is restricted to read-only. Changes can't be made to the community. Read Write—Management access is read-write. Changes can be made to the device configuration, but not to the community. SNMP Admin—User has access to all device configuration options, and permissions to modify the community. SNMP Admin is equivalent to Read Write for all MIBs except for the SNMP MIBs. SNMP Admin is required for access to the SNMP MIBs. • View Name—Select an SNMP view (a collection of MIB subtrees to which access is granted).
Advanced	Select this type for a selected community. • Group Name—Select an SNMP group that determines the access rights.

Step 4 Click **Apply**. The SNMP Community is defined, and the Running Configuration is updated.

Trap Settings

The Trap Settings page enables configuring whether SNMP notifications are sent from the device, and for which cases.

To define trap settings, follow these steps:

Procedure

Step 1 Click **SNMP** > **Trap Settings**.

Step 2 Select **Enable** for SNMP Notifications to specify that the device can send SNMP notifications.

Step 3 Select **Enable** for Authentication Notifications to enable SNMP authentication failure notification.

Step 4 Click **Apply**. The SNMP Trap settings are written to the Running Configuration file.

Notification Recipients SNMPv1,2

The notification recipients enable configuring the destination to which SNMP notifications are sent, and the types of SNMP notifications that are sent to each destination (traps or informs). An SNMP notification is a message sent from the device to the SNMP management station indicating that a certain event has occurred, such as a link up/down.

It is also possible to filter certain notifications. This can be done by creating a filter in the Notification Filter, on page 374 and attaching it to an SNMP notification recipient. The notification filter enables filtering the type of SNMP notifications that are sent to the management station based on the OID of the notification that is about to be sent.

To define a recipient in SNMPv1,2:

Procedure

Step 1 Click **SNMP** > **Notification Recipients SNMPv1,2**.

This page displays recipients for SNMPv1,2.

Step 2 Enter the following fields:

- Informs IPv4 Source Interface—Select the source interface whose IPv4 address will be used as the source IPv4 address in inform messages for communication with IPv4 SNMP servers.
- Traps IPv4 Source Interface—Select the source interface whose IPv6 address will be used as the source IPv6 address in trap messages for communication with IPv6 SNMP servers.
- Informs IPv6 Source Interface—Select the source interface whose IPv4 address will be used as the source IPv4 address in inform messages for communication with IPv4 SNMP servers.
- Traps IPv6 Source Interface—Select the source interface whose IPv6 address will be used as the source IPv6 address in trap messages for communication with IPv6 SNMP servers.

Note
If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

Step 3 Click **Add.**

Step 4 Enter the parameters.

- Server Definition—Select whether to specify the remote log server by IP address or name.
- IP Version—Select either IPv4 or IPv6.
- IPv6 Address Type—Select either Link Local or Global.
  - Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication on the local network only. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.

- Link Local Interface—If the IPv6 address type is Link Local, select whether it's received through a VLAN or ISATAP.
- Recipient IP Address/Name—Enter the IP address or server name of where the traps are sent.
- UDP Port—Enter the UDP port used for notifications on the recipient device.
- Notification Type—Select whether to send Traps or Informs. If both are required, two recipients must be created.
- Timeout—Enter the number of seconds the device waits before resending informs.
- Retries—Enter the number of times that the device resends an inform request.
- Community String—Select from the pull-down the community string of the trap manager. Community String names are generated from those listed in the SNMP Communities, on page 369.
- Notification Version—Select the trap SNMP version. Either SNMPv1 or SNMPv2 may be used as the version of traps, with only a single version enabled at a time.
- Notification Filter—Select to enable filtering the type of SNMP notifications sent to the management station. The filters are created in the Notification Filter, on page 374.
- Filter Name—Select the SNMP filter that defines the information contained in traps (defined in the Notification Filter, on page 374).

Step 5 Click **Apply**. The SNMP Notification Recipient settings are written to the Running Configuration file.

Notification Recipients SNMPv3

To define a recipient in SNMPv3:

Procedure

Step 1 Click **SNMP** > **Notification Recipients SNMPv3**.

Step 2 Configure the following settings:

- Informs IPv4 Source Interface—From the drop-down list, select the source interface whose IPv4 address will be used as the source IPv4 address in inform messages for communication with IPv4 SNMP servers.
- Traps IPv4 Source Interface—From the drop-down list, select the source interface whose IPv6 address will be used as the source address in trap messages.
- Informs IPv6 Source Interface—From the drop-down list, select the source interface whose IPv4 address will be used as the source IPv4 address in inform messages for communication with IPv4 SNMP servers.
- Traps IPv6 Source Interface—From the drop-down list, select the source interface whose IPv6 address will be used as the source address in trap messages.

Step 3 Click **Add.**

Step 4 Enter the parameters.

- Server Definition—Select whether to specify the remote log server by IP address or name.
- IP Version—Select either IPv4 or IPv6.
- IPv6 Address Type—Select the IPv6 address type (if IPv6 is used). The options are:
  - Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, isn't routable, and can be used for communication on the local network only. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- Link Local Interface—Select the link local interface (if IPv6 Address Type Link Local is selected) from the pull-down list.
- Recipient IP Address/Name—Enter the IP address or server name of where the traps are sent.
- UDP Port—Enter the UDP port used to for notifications on the recipient device.
- Notification Type—Select whether to send traps or informs. If both are required, two recipients must be created.
- Timeout—Enter the amount of time (seconds) the device waits before resending informs/traps. Time out: Range 1-300, default 15
- Retries—Enter the number of times that the device resends an inform request. Retries: Range 1-255, default 3
- User Name—Select from the drop-down list the user to whom SNMP notifications are sent. In order to receive notifications, this user must be defined on the page, and its engine ID must be remote.
- Security Level—Select how much authentication is applied to the packet.

  Note
  The Security Level here depends on which User Name was selected. If this User Name was configured as No Authentication, the Security Level is No Authentication only. However, if this User Name has been assigned with Authentication and Privacy rights, the security level can be either No Authentication, or Authentication Only, or Authentication and Privacy.

  The options are:
  - No Authentication—Indicates that the packet is not authenticated or encrypted.
  - Authentication—Indicates that the packet is authenticated but not encrypted.
  - Privacy—Indicates that the packet is both authenticated and encrypted.
- Notification Filter—Select to enable filtering the type of SNMP notifications sent to the management station.
- Filter Name—Select the SNMP filter that defines the information contained in traps.

Step 5 Click **Apply**. The SNMP Notification Recipient settings are written to the Running Configuration file.

Notification Filter

The Notification Filter page enables configuring SNMP notification filters and Object IDs (OIDs) that are checked. The notification filter enables filtering the type of SNMP notifications that are sent to the management station based on the OID of the notification to be sent.

To define a notification filter:

Procedure

Step 1 Click **SNMP** > **Notification Filter**.

The Notification Filter Table contains notification information for each filter. The table is able to filter notification entries by Filter Name. The Object ID Subtree Filter displays the current status of each configured filter.

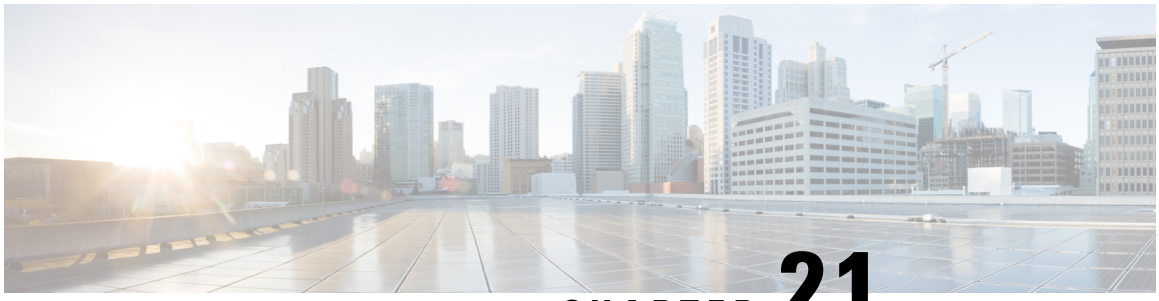
Step 2 Click **Add**.

Step 3 Enter the parameters.

- Filter Name—Enter a name between 0-30 characters.
- Object ID Subtree—Select the node in the MIB tree that is included or excluded in the selected SNMP filter. The options to select the object are as follows:
  - Select from List—Enables you to navigate the MIB tree. Press the Up arrow to go to the level of the selected node's parent and siblings; press the Down arrow to descend to the level of the selected node's children. Click nodes in the view to pass from one node to its sibling. Use the scrollbar to bring siblings in view.
  - Object ID—Select this option to include the entered object identifier in the view, if the Include in filter option is selected.

Step 4 Select or deselect **Include in filter.** If this is selected, the selected MIBs are included in the filter, otherwise they are excluded.

Step 5 Click **Apply**. The SNMP views are defined and the running configuration is updated.



CHAPTER 21

Annex

This chapter contains general topics that may only apply to certain models of the Cisco Business switches.

- Managing a Stack of Switches, on page 375
- Link Aggregation, on page 382
- UDLD , on page 384
- Smartport Overview, on page 385
- VLAN Description, on page 386
- Troubleshooting Link Flapping, on page 391
- Spanning Tree Protocol, on page 393
- RSPAN Configuration, on page 395
- Multicast, on page 396
- 802_1x Overview, on page 400
- Mode Behavior, on page 406
- DHCPv4 Types and Interactions, on page 407
- IPv6 First Hop Security, on page 412
- Secure Sensitive Data Management, on page 420
- Secure Shell, on page 421
- QoS, on page 422
- SNMP, on page 424

Managing a Stack of Switches

Switches can either function on their own, or they can be connected into a stack of switches. By default, a device is always stackable, but has no stack port. All ports on the switches are network ports by default. You can look at a switch without any stack port as the active unit in a stack of only itself. You can also look at a switch without any stack port as a standalone switch. To stack two or more devices, reconfigure the desired network ports as stack ports in the switches and connect the switches with the resulting stack ports in a ring or chain topology.

The switches (units) in a stack are connected through stack ports. These switches are then collectively managed as a single logical switch. In some cases, stack ports can become members in Link Aggregation Groups (LAGs) increasing the bandwidth of the stack port.

The stack is based on a model of a single active/standby and multiple members. A stack provides the following benefits:

- Network capacity can be expanded or contracted dynamically. By adding a unit, the administrator can dynamically increase the number of ports in the stack while maintaining a single point of management. Similarly, units can be removed to decrease network capacity.
- The stacked system supports redundancy in the following ways:
  - The standby unit becomes the active of the stack if the original active fails.
  - The stack system supports two types of topologies: chain and ring. In ring topology, if one of the stack ports fails, the stack continues to function in chain topology.
  - A process known as Fast Stack Link Failover is supported on the ports in a ring stack to reduce the duration of data packet loss when one of the stack ports link fails. Until the stack recovers to the new chain topology, a stack unit loops back the packets that are supposed to be sent through its failed stacking port, and transmits the looped back packets through its remaining stacking port to the destinations. During Fast Stack Link failover, the active/standby units remain active and functioning.

Types of Units in Stack

A stack consists of a maximum of eight units. A unit in a stack is one of the following types:

- **Active**—The active unit's ID must be either 1 or 2. The stack is managed through the active unit that manages itself, the stand by unit and the member units.
- **Stand by**—If the active unit fails, the stand by unit assumes the active role(switchover). The stand by unit's ID must be either 1 or 2.
- **Member**—These units are managed by the active unit.

In order for a group of units to function as a stack, there must be an active-enabled unit. When the active-enabled unit fails, the stack continues to function as long as there is a stand by unit (the main unit that assumes the active role).If the stand by unit fails, in addition to the active unit, and the only functioning units are the member units. These also stop functioning after one minute. This means for example, that if after 1 minute, you plug in a cable to one of the member units that was running without an active, the link will not come up.

Backward Compatibility of Number of Units in Stack

The stackable switches support anywhere from four units to eight units. This varies based on the switch model. Upgrading from and earlier software release can be done without changing the configuration files. When a firmware version, which does not support the hybrid stack modes is loaded to the stack and the stack is rebooted, the stack reverts to Native Stack mode. When a device in Hybrid stack mode is loaded with a firmware version that does not support Hybrid stack mode, its system mode reverts to the default system mode. If a stack's unit IDs were manually-configured, those units whose ID is greater than 4 are switched to auto numbering.

Stack Topology

The units in a stack can be connected in one of the following types of topologies:

- Chain Topology—Each unit is connected to the neighboring unit, but there is no cable connection between the first and last unit.

- Ring Topology—Each unit is connected to the neighboring unit. The last unit is connected to the first unit. The following shows a ring topology of an eight-unit stack:

A ring topology is more reliable than a chain topology. The failure of one link in a ring does not affect the function of the stack, whereas the failure of one link in a chain connection might cause the stack to be split.

Topology Discovery

A stack is established by a process called topology discovery. This process is triggered by a change in the up/down status of a stack port. The following are examples of events that trigger this process:

- Changing the stack topology from a ring to a chain
- Merging two stacks into a single stack
- Splitting the stack
- Inserting other member units to the stack, for instance because the units previously disconnected from the stack due to a failure. This can happen in a chain topology if a unit in the middle of the stack fails.

During topology discovery, each unit in a stack exchanges packets, which contain topology information. After the topology discovery process is completed, each unit contains the stack mapping information of all units in the stack.

Unit ID Assignment

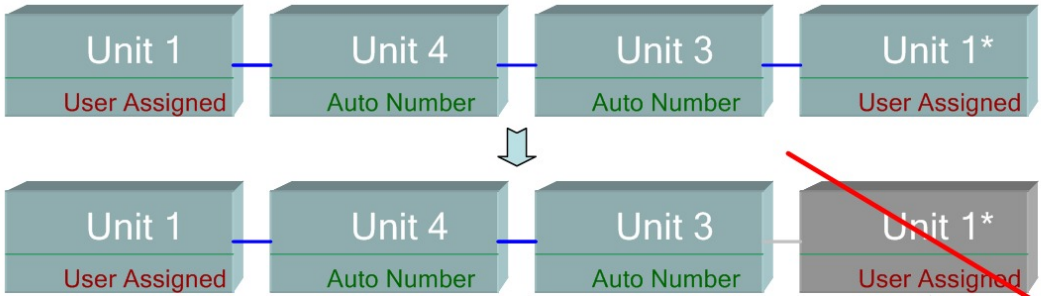
After topology discovery is completed, each unit in a stack is assigned a unique unit ID. The unit ID is set in the System Mode and Stack Management page in one of the following ways:

- **Automatically (Auto)** —The Unit ID is assigned by the topology discovery process. This is the default setting.
- **Manually**—The unit ID is manually set to an integer from 1-8.

Duplicate Unit IDs

If you assign the same unit ID to two separate units, only one of them can join the stack with that unit ID. If auto numbering has been selected, the duplicate unit is assigned a new unit number. If auto numbering was not selected, the duplicate unit is shut down. The following shows a case where two units were manually assigned the same unit ID. Unit 1 does not join the stack and is shut down. It did not win the active selection process between the active-enabled units (1 or 2).

Duplicate Unit Shut Down



Active Selection Process

The active unit is selected from the active-enabled units (1 or 2). The factors in selecting the active unit are taken into account in the following priority:

- **Force Active**—If Force Active is activated on a unit, it is selected.
- **System Up Time**—The active-enabled units exchange up-time, which is measured in segments of 10 minutes. The unit with the higher number of segments is selected. If both units have the same number of time segments,and the unit ID of one of the units was set manually while the other unit's unit ID was set automatically, the unit with the manually-defined unit ID is selected; otherwise the unit with the lowest unit ID is selected. If both units IDs are the same, the unit with the lowest MAC address is chosen.

Note The up time of the stand by unit is retained when it is selected as active in the switch failover process.

- **Unit ID**—If both units have the same number of time segments, the unit with the lowest unit ID is selected.
- **MAC Address**—If both units IDs are the same, the unit with the lowest MAC address is chosen.

Note For a stack to operate, it must have an active unit. An active unit is defined as the main unit that assumes the active role. The stack must contain a unit 1 and/or unit 2 after the active selection process. Otherwise, the stack and all its units are partially shut down, not as a complete power-off, but with traffic-passing capabilities halted

Stack Changes

This section describes various events that can cause a change to the stack. A stack topology changes when one of the following occurs:

- One or more units are connecting and/or disconnecting to and from the stack.
- Any of its stack ports has a link up or down.
- The stack changes between ring and chain formation.

When units are added or removed to and from a stack, it triggers topology changes, master election process, and/or unit ID assignment.

Connecting a New Unit

When a unit is inserted into the stack, a stack topology change is triggered. The unit ID is assigned (in case of auto numbering), and the unit is configured by the active unit.

One of the following cases can occur when connecting a new unit to an existing stack:

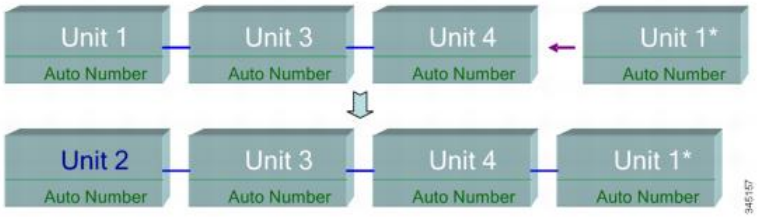
- No duplicate unit IDs exist.
    - Units with user-defined IDs retain their unit ID.

- Units with automatically-assigned IDs retain their unit ID.
- Factory default units receive unit IDs automatically, beginning from the lowest available ID.

- One or more duplicate unit IDs exist. Auto numbering resolves conflicts and assigns unit IDs. In case of manual numbering, only one unit retains its unit ID and the other(s) are shutdown.
- The number of units in the stack exceeds the maximum number of units allowed. The new units that joined the stack are shut down, and a SYSLOG message is generated and appears on the master unit

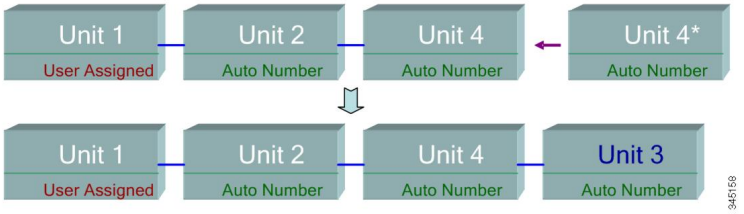
The following shows an example of auto numbering when an active-enabled unit joins the stack. There are two units with unit ID = 1. The active selection process selects the best unit to be the active unit. The best unit is the unit with the higher uptime in segments of 10 minutes. The other unit is made the backup

Auto-numbered Active-enabled Unit



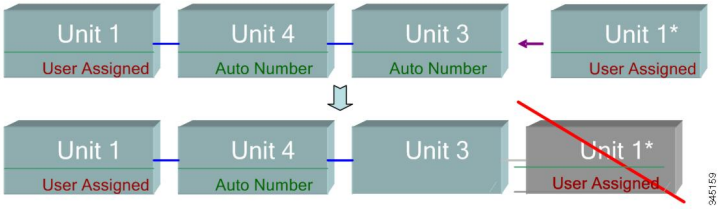
The following shows an example of auto numbering when a new unit joins thes tack. The existing units retain their ID. The new unit receives the lowest available ID.

Auto Number Unit



The following shows what happens when a user-assigned, active-enabled unit with Unit ID 1 joins a stack that already has an active unit with user-assigned unit ID1. The newer Unit 1 does not join the stack and is shutdown.

User-assigned Active-enabled Unit



Unit Failure in Stack

If the active unit fails, then the standby unit will take over the primary role and continues to operate the stack normally.

For the standby switch to be able to take the place of the active switch, both units remain on reserve at all times. When on reserve mode, the active switch and its standby switches are synchronized with a static configuration (contained in both the Startup and Running configuration files). The standby switch configuration file remains on the previous active switch.

Dynamic process-state information, such as the STP state table, dynamically-learned MAC addresses, dynamically-learned Smartport types, MAC Multicast tables, LACP, and GVRP are not synchronized. When an active switch is being configured, it synchronizes with the standby unit immediately. Synchronization is performed as soon as a command is executed. This is transparent.

When an active switch is being configured, it synchronizes the backup immediately. Synchronization is performed as soon as a command is executed. This is transparent.

If a unit is inserted into a running stack, and is selected as a standby unit, the active switch synchronizes it so that it has an up-to date configuration, and then generates a SYNC COMPLETE SYSLOG message. This is a unique SYSLOG message that appears only when standby is converging with the active unit, and looks like this: %DSYNCH-I-SYNCH_SUCCEEDED: Synchronization with unit 2 is finished successfully.

Active / Standby Switchover

When a active switch fails on the stack, a switchover occurs. The standby unit becomes the active, and all of its processes and protocol stacks are initialized to take responsibility for the entire stack. As a result, there is temporarily no traffic forwarding in this unit, but member units remain active.



Note When STP is used and the ports are in link up, the STP port's state is temporarily Blocking, and it cannot forward traffic or learn MAC addresses. This is to prevent spanning tree loops between active units.

Member Unit Handling

While the standby unit becomes the active switch, the member units remain active and continue to forward packets based on the configuration from the original active switch. This minimizes data traffic interruption in units. After the standby unit has completed the transition to the active state, it initializes the member units one at a time by performing the following operations:

- Clear and reset the configuration of the member unit to default (to prevent an incorrect configuration from the new active unit). As a result, there is no traffic forwarding on the member unit.
- Apply related user configurations to the member unit.
- Exchange dynamic information such as port STP state, dynamic MAC addresses, and link up/down status between the new active and member unit. Packet forwarding on the member unit resumes after the state of its ports are set to forwarding by the active switch according to STP.



Note Packet flooding to unknown Unicast MAC addresses occurs until the MAC addresses are learned or relearned.

Reconnecting the Original Active Unit after Failover

After failover, if the original active switch is connected again, the active selection process is performed. If the original active switch (unit 1) is reselected to be the active unit, the current active switch (unit 2, which was the original backup unit) is rebooted and becomes the backup once again.



Note During active unit failover, the uptime of the standby unit is retained.

Software Auto Synchronization in a Stack

All units in the stack must run the same software version (firmware and boot code). Each unit in a stack automatically downloads firmware and boot code from the active unit if the firmware and/or boot code that the unit and the active are running is different. The unit automatically reboots itself to run the new version.

Stack Ports

All ports on the device are network (uplink) ports by default. To connect units, you must change the types of the ports to be used to connect the devices as stack ports. These ports are used to transfer data and protocol packets among the units

Stack Port Link Aggregation

When two neighboring units are connected, the stack ports connecting them are automatically assigned to a stack LAG. This feature enables increasing the stack bandwidth of the stack port beyond that of a single port. There can be up to two stack LAGs per unit.

The stack LAG can be composed of between two and up to the maximum number of stack ports depending on the unit type.

Stack Port States

Stack ports can be in one of the following states:

- Down—Port operational status is down or stack port operational status is up, but traffic cannot pass on the port.
- Active—Stack port was added to a stack LAG whose stack port operational status is up and traffic can pass on the port and it is a member of a stack LAG.
- Standby—Stack port operational status is up and bidirectional traffic can pass on the port, but the port cannot be added to a stack LAG, and the port does not transmit traffic. Possible reasons for a port being in standby are:
    - Stack ports with different speeds are used to connect a single neighbor.

Backwards Compatibility

The following modes have been expanded in the current software version of the device. Care must be taken when using these features in previous software versions:

- **Stack Port LAG**—If a unit whose software supports stack ports in LAGs is connected to a unit whose software does not support stack ports in LAGs, the stack port connecting the units is not made a member

of the stack LAG. The units are connected through the stack ports, and the active stack unit copies its software to the other unit. The software copied depends on the unit which becomes the active unit.

- **Queues Mode**—This mode can be changed from 4 QoS queues to 8 QoS queues. There is no issue when upgrading from previous software versions that did not support 8 queues, since the 4-queue mode is the default queues mode in the current software version. However, when changing the queues mode to 8 queues, the configuration must be examined and adjusted to meet the desired QoS objectives with the new queues mode. Changing the queues mode takes effect after rebooting the system. Queue-related configuration that conflicts with the new queues mode is rejected.
- **Stacking Mode**—The Stacking mode has been expanded to include hybrid stacking modes. There is no problem in upgrading from previous software versions, since the device will boot with the existing stacking mode (Native Stacking mode). If you want to downgrade software from a device that was configured in a hybrid stacking mode to a software version that does not support hybrid stacking, configure the device to Native Stacking mode first.

Physical Constraints for Stack LAGs

- A stack LAG must contain ports of the same speed.
- When attempting to connect a unit to a stack whose topology is not a ring/chain (for example, trying to connect a unit to more than two neighboring units - star topology), only two stack LAGs can be active, the remainder of the stack ports are set to standby mode (inactive).

Auto Selection of Port Speed

The stacking cable type is discovered automatically when the cable is connected to the port (auto-discovery is the default setting). The system automatically identifies the stack cable type and selects the highest speed supported by the cable and the port.

A SYSLOG message (informational level) is displayed when the cable type is not recognized.

Link Aggregation

Overview

Link Aggregation Control Protocol (LACP) is part of the IEEE specification (802.3az) that enables you to bundle several physical ports together to form a single logical channel (LAG). LAGs multiply the bandwidth, increase port flexibility, and provide link redundancy between two devices. Link aggregation allows you combine multiple Ethernet links to a single link between two network devices. The most common combinations involve connecting a switch to another switch, a server, a network attached storage (NAS) device, or a multiport WiFi access point.

Network devices and management functions treat the link aggregation group (LAG) of multiple Ethernet connections as a single link. For example, you can include a LAG in a virtual local area network (VLAN). You can also configure more than one LAG on the same switch, or add more than two Ethernet links to the same LAG (the maximum number of links per LAG depends on your device).

Some network devices support Link Aggregation Control Protocol (LACP), which helps to prevent errors in the link aggregation setup process.

Link Aggregation Benefits

Link Aggregation offers the following benefits:

- Increased reliability and availability- If one of the physical links in the LAG goes down, traffic reassigned to another physical links.
- Better use of physical resources- Traffic can be load-balanced across the physical links.
- Increased bandwidth- The aggregated physical links deliver higher bandwidth than each individual link.
- Cost effectiveness- A physical network upgrade can be expensive, especially if it requires new cable runs. Link aggregation increases bandwidth without requiring new equipment.

Link Aggregation Set Up

The following instructions describe in general terms how to set up link aggregation between two devices in your network.

Procedure

Step 1 Make sure that both devices support link aggregation.

Step 2 Configure the LAG on each of the two devices.

Step 3 Make sure that the LAG that you create on each device has the same settings for port speed, duplex mode, flow control, and MTU size.

Step 4 Make sure that all ports that are members of a LAG have the same virtual local area network (VLAN) memberships. If you want to add a LAG to a VLAN, set up the LAG first and then add the LAG to the VLAN; do not add individual ports.

Warning
Do not connect the devices to each other using more than one Ethernet cable until after you set up the LAG on each device. If you form multiple connections between the two devices and neither device has loop prevention, you create a network loop. Network loops can slow or stop normal traffic on your network.

Step 5 Note the ports on each device to which you add the LAG, and make sure that you connect to the correct ones. The LAG issues an alert and rejects the configuration if the port members have different settings for port speed, duplex mode, or MTU size, or if you accidentally connect ports that are not members of the LAG.

Step 6 Use Ethernet or fiber cable to connect the ports that you added to the LAG on each device.

Step 7 Verify that the port LED for each connected port on each switch is blinking green.

Step 8 Verify in the admin interface for each device that the link is up.

Configure LAG Load Balance

Procedure

Step 1 Log in to the Cisco switch by entering the **Username** and **Password**. Click **Log In**. By default the username and password are *cisco*, but since you are working on an existing network, you should have your own username and password. Enter those credentials instead.

Step 2 Navigate to **Port Management > LAG Management** and select the Load Balance Algorithm option. You can select either *MAC Address*, or *IP/MAC Address*. Click **Apply**.

Note
By default, **MAC Address** is the option selected for *Load Balance Algorithm*.

Step 3 Next, the *Success* notification should appear on the screen. Click **File Operations** to save the configuration on the switch to startup configuration.

Step 4 The *File Operations* page will open. Verify that the *Source File Name* is selected as **Running Configuration** and *Destination File Name* is selected as **Startup Configuration**. Click **Apply** to save the configuration.

UDLD

Overview

Unidirectional Link Detection (UDLD) is a Layer 2-protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to detect unidirectional links. A unidirectional link occurs whenever traffic from a neighboring device is received by the local device, but traffic from the local device is not received by the neighbor.

The purpose of UDLD is to detect ports on which the neighbor does not receive traffic from the local device (unidirectional link) and to shut down those ports. All connected devices must support UDLD for the protocol to successfully detect unidirectional links. If only the local device supports UDLD, it is not possible for the device to detect the status of the link. In this case, the status of the link is set to undetermined. The user can configure whether ports in the undetermined state are shut down or merely trigger notifications.

How UDLD Works

When UDLD is enabled on a port, the following actions are performed:

- UDLD initiates the detection state on the port.
    - In this state, UDLD periodically sends messages on every active interface to all neighbors. These messages contain the device ID of all known neighbors. It sends these messages according to a user-defined message time.
- UDLD receives UDLD messages from neighboring devices. It caches these messages until the expiration time (3 times message time) has passed. If a new message is received before the expiration time, the information in that message replaces the previous one.

- When the expiration time expires, the device does the following with the information received:
  - If the neighbor message contains the local device ID—The link status of the port is set to bidirectional.
  - If the neighbor message does not contain the local device ID—The link status of the port is set to unidirectional, and the port is shut down.
- If UDLD messages are not received from a neighboring device during the expiration time frame, the link status of the port is sent to undetermined and the following occurs:
  - Device is in normal UDLD mode: A notification is issued.
  - Device is in aggressive UDLD mode. The port is shut down.

While the interface is in the bidirectional or the undetermined state, the device periodically sends a message each message time seconds. The above steps are performed over and over.

Usage Guidelines

Cisco does not recommend enabling UDLD on ports that are connected to devices on which UDLD is not supported or disabled. Sending UDLD packets on a port connected to a device that does not support UDLD causes more traffic on the port without providing benefits.

In addition, consider the following when configuring UDLD:

- Set the message time according to how urgent it is to shut down ports with a unidirectional link. The lower the message time, the more UDLD packets are sent and analyzed, but the sooner the port is shut down if the link is unidirectional.
- If you want UDLD to be enabled on a copper port, you must enable it per port. When you globally enable UDLD, it is only enabled on fiber ports.
- Set the UDLD mode to normal when you do not want to shut down ports unless it is known for sure that the link is unidirectional.
- Set the UDLD mode to aggressive when you want both unidirectional and bidirectional link loss.

Smartport Overview

The Smartport feature provides a convenient way to save and share common configurations. By applying the same Smartport macro to multiple interfaces, the interfaces share a common set of configurations. A Smartport macro is a script of CLI (Command Line Interface) commands

A Smartport macro can be applied to an interface by the macro name, or by the Smartport type associated with the macro. Applying a Smartport macro by macro name can be done only through CLI.

There are two ways to apply a Smartport macro by Smartport type to an interface:

- Static Smartport—You manually assign a Smartport type to an interface. The result is the corresponding Smartport macro is applied to the interface.
- Auto Smartport—Auto Smartport waits for a device to be attached to the interface before applying a configuration. When a device is detected from an interface, the Smartport macro (if assigned) that corresponds to the Smartport type of the attaching device is automatically applied.

A Smartport is an interface to which a built-in (or user-defined) macro may be applied. These macros are designed to provide a means of quickly configuring the device to support the communication requirements and utilize the features of various types of network devices. The network access and QoS requirements vary if the interface is connected to an IP phone, a printer, or a router and/or Access Point (AP).

VLAN Description

Each VLAN is assigned a VLAN ID (VID) with a value ranging from 1 to 4094. A VLAN member is a port on a device in a bridged network that may send and receive data from the VLAN. If all packets headed for that port into the VLAN have no VLAN tag, the port is an untagged member of the VLAN. If all packets headed for that port into the VLAN include a VLAN tag, that port is a tagged member of the VLAN. A port can only belong to one untagged VLAN, although it can belong to several tagged VLANs.

In VLAN Access mode, a port can only belong to one VLAN. The port can be part of one or more VLANs if it is in General or Trunk mode. VLANs are used to solve security and scalability problems. VLAN traffic stays within the VLAN and is terminated at VLAN devices. It also simplifies network configuration by conceptually linking devices without requiring them to be physically relocated.

A four-byte VLAN tag is applied to each Ethernet frame if it is VLAN-tagged. The tag comprises a VLAN ID ranging from 1 to 4094, as well as a VLAN Priority Tag (VPT) ranging from 0 to 7 When a frame enters a VLAN-aware device, the four-byte VLAN tag in the frame is used to classify it as belonging to a VLAN. The frame is classified to the VLAN based on the PVID (Port VLAN Identifier) defined at the ingress port where the frame is received if there is no VLAN tag in the frame or if the packet is merely priority-tagged. If Ingress Filtering is enabled and the ingress port is not a member of the VLAN to which the packet belongs, the frame is dropped at the ingress port. Only if the VID in the VLAN tag is 0 is a frame considered priority-tagged. Frames that belong to a VLAN stay in the VLAN.

This is accomplished by transmitting or forwarding a frame only to members of the target VLAN's egress ports. A VLAN's egress port can be either tagged or untagged.

The egress port's role is as follows:

- If the egress port is a tagged member of the target VLAN and the original frame does not include a VLAN tag, the egress port adds a VLAN tag to the frame.
- If the egress port is an untagged member of the target VLAN and the original frame has a VLAN tag, the VLAN tag is removed from the frame.

VLAN Roles

Layer 2 is where VLANs work. All VLAN traffic (Unicast, Broadcast, and Multicast) is contained within the VLAN. Over the Ethernet MAC layer, devices connected to separate VLANs do not have direct connectivity. Only Layer 3 routers allow devices from different VLANs to interact with one another. If each VLAN represents an IP subnet, an IP router is necessary to route IP traffic between them.

The IP router could be a standard router with only one VLAN connected to each of its ports. VLAN untagged traffic to and from a standard IP router is required. Each of the IP router's interfaces can connect to one or more VLANs, making it a VLAN-aware IP router. Traffic to and from a VLAN-aware IP router can be VLAN tagged or untagged.

Generic VLAN Registration Protocol is used by adjacent VLAN-aware devices to communicate VLAN information (GVRP). VLAN information is thus conveyed across a bridged network. Based on the GVRP information exchanged by devices, VLANs can be formed statically or dynamically on a device. A VLAN

can be static or dynamic (thanks to the GVRP), but not both at the same time. Refer to the GVRP Settings section for further information about GVRP.

QinQ

QinQ provides isolation between service provider networks and customers' networks. The device is a provider bridge that supports port-based c-tagged service interface.

With QinQ, the device adds an ID tag known as Service Tag (S-tag) to forward packets into the provider network. The S-tag is used to segregate traffic between various customers, while preserving the customer VLAN tags.

Customer traffic is encapsulated with an S-tag with TPID 0x8100, regardless of whether it was originally c-tagged or untagged. The S-tag enables this traffic to be treated as an aggregate within a provider bridge network, where the bridging is based on the S-tag VID (S-VID) only.

The S-Tag is preserved while traffic is forwarded through the network service provider's infrastructure, and is later removed by an egress device.

An additional benefit of QinQ is that there is no need to configure customers' edge devices.

Private VLAN

The Private VLAN feature provides layer-2 isolation between ports. This means that at the level of bridging traffic, as opposed to IP routing, ports that share the same Broadcast domain cannot communicate with each other. The ports in a private VLAN can be located anywhere in the layer 2 network, meaning that they do not have to be on the same switch. The private VLAN is designed to receive untagged or priority-tagged traffic and transmit untagged traffic.

The following types of ports can be members in a private VLAN:

- Promiscuous—A promiscuous port can communicate with all ports of the same private VLAN. These ports connect servers and routers.
- Community (host)—Community ports can define a group of ports that are member in the same Layer 2 domain. They are isolated at Layer 2 from other communities and from isolated ports. These ports connect host ports.
- Isolated (host)—An isolated port has complete Layer 2 isolation from the other isolated and community ports within the same private VLAN. These ports connect host ports.

The following types of private VLANs exist:

- Primary VLAN—The primary VLAN is used to enable Layer 2 connectivity from promiscuous ports to isolated and to community ports. There can only be a single primary VLAN per private VLAN.
- Isolated VLAN (also known as a Secondary VLAN)—An isolated VLAN is used to enable isolated ports to send traffic to the primary VLAN. There can only be a single, isolated VLAN per private VLAN.
- Community VLAN (also known as a Secondary VLAN)—To create a sub-group of ports (community) within a VLAN, the ports must be added a community VLAN. The community VLAN is used to enable Layer 2 connectivity from community ports to promiscuous ports and to community ports of the same community. There can be a single community VLAN for each community and multiple community VLANs can coexist in the system for the same private VLAN).

Host traffic is sent on isolated and community VLANs, while server and router traffic is sent on the primary VLAN.

Shared MAC address learning exists between all the VLANs that are members in the same private VLAN (although the switch supports independent VLAN learning). This enables Unicast traffic, despite the fact that host MAC addresses are learned by isolated and community VLANs, while routers and server MAC addresses are learned by the primary VLAN.

A private VLAN-port can only be added to one private VLAN. Other port types, such as access or trunk ports, can be added to the individual VLANs that make up the private VLAN (since they are regular 802.1Q VLANs).

A private VLAN can be configured to span across multiple switches by setting inter-switch ports as trunk ports and adding them to all VLANs in the private VLAN. Inter-switch trunk ports send and receive tagged traffic of the private VLAN's various VLANs (primary, isolated and the communities).

Configure a VLAN on a Switch

Virtual Local Area Network (VLAN) creation allows you to make separate broadcast domains on a switch. The broadcast domains can associate with one another with the help of a Layer 3 device such as a router. A VLAN is mainly used to form groups among the hosts regardless of where the hosts are physically located. Thus, a VLAN improves security with the help of group formation among the hosts. When a VLAN is created, it has no effect until that VLAN is attached to at least one port either manually or dynamically. One of the most common reasons to set up a VLAN is to set up a separate VLAN for voice, and a separate VLAN for data. This directs the packets for both types of data despite using the same network.

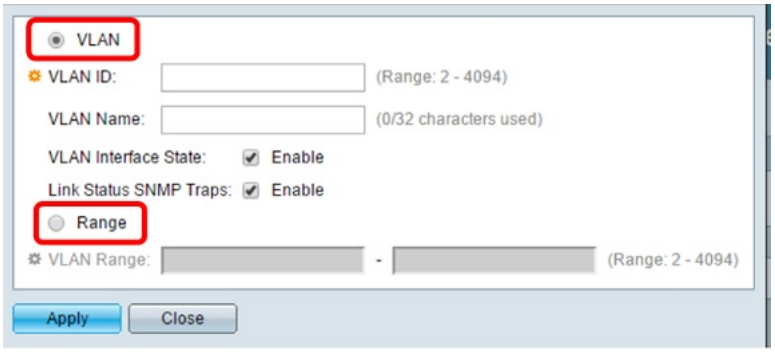
Create a VLAN

Procedure

Step 1 Log in to the web-based utility and choose **VLAN Management > VLAN Settings**.

Step 2 Under the VLAN Table area, click **Add** to create a new VLAN.

Step 3 VLAN can be added in two different methods as shown by the options below. Choose a radio button that corresponds to the desired method:



- **VLAN** — Use this method to create a specific VLAN.
- **Range** — Use this method to create a range VLANs.

Step 4 If you chose VLAN in Step 3, enter the VLAN ID in the VLAN ID field. The range must be between 2 to 4094.

Step 5 In the VLAN Name field, enter a name for the VLAN. For this example, the VLAN Name will be Accounting. Up to 32 characters may be used.

Step 6 Check the VLAN Interface State check box to enable the VLAN interface state; it is already checked by default. If not, the VLAN will be effectively shut down, and nothing will be able to be transmitted or received through the VLAN.

Step 7 Check the Link Status SNMP Traps check box if you want to enable the generation of SNMP traps. This is enabled by default.

Step 8 If you chose Range in Step 3, enter the range of the VLANs in the VLAN Range field. The available range is 2–4094. For this example, the VLAN Range is from 3 to 52.

Note
Up to 100 VLANs can be created at a time.

Step 9 Click **Apply**.

GVRP Configuration

GVRP is supported only on COS switches. GVRP will run only on 802.1Q trunk ports and is used primarily to prune traffic from VLANs that does not need to be passed between trunking switches. Use the following steps to configure GVRP. To ensure that port remains in General mode it is strongly advised to disable smartport macro auto on each interface participating in GVRP.

Procedure

Step 1 Configure the switch with the desired VLANs. For example, you can configure the following settings:

- Switch 1 can be assigned a VLAN ID of 1 as the default, then 300, 400 and 500.
- Switch 2 can be assigned a VLAN ID of 1 as the default.
- Switch 3 can be assigned a VLAN ID of 1 as the default, then 100 and 200.

Step 2 To enable GVRP on an interface, it must be configured in General Mode, otherwise the switch will not send any GARP messages.

Step 3 Enable GVRP globally. By default GVRP is not enabled for the switch. You must first enable GVRP on the switch before you can configure the 802.1Q ports for GVRP operation.

Step 4 Configure the port for 802.1Q operation. GVRP will run only on ports that are configured for 802.1Q trunking.

Step 5 Configure the port GVRP. GVRP must be configured on both sides of the trunk to work correctly.

Step 6 (Optional) Configure the port registration mode. By default GVRP ports are in **normal** registration mode. These ports use GVRP join messages from neighboring switches to prune the VLANs running across the 802.1Q trunk link. If the device on the other side is not capable of sending GVRP messages, or if you do not want to allow the switch to prune any of the VLANs, use the **fixed** mode. Fixed mode ports will forward for all VLANs that exist in the switch database. Ports in **forbidden** mode forward only for VLAN 1.

Voice VLAN Configuration

This troubleshooting tip is for Voice VLAN configuration.

Procedure

Step 1 Create a VLAN on the switch. For example, if the data VLAN is set at 2 and the Voice VLAN is set at 5, then assign VLAN 5 in the Auto Voice VLAN tab.

Step 2 Make sure that you see the operational Voice VLAN set to 5.

Step 3 Change Display Mode from **Basic** to **Advanced**.

Step 4 Next, in the Interface Settings under VLAN Management, change the port mode from **Access** to **Trunk**.

Step 5 Next, under Port to VLAN Membership, set the data VLAN as untagged and Voice VLAN as tagged on the port that is connected to the IP phones. Do the same for the desktops and laptops that are connected to the IP phones.

Step 6 Go to IP configuration > IPv4 Interface and assign an IP to both VLAN 2 and VLAN 5.

Step 7 Create a DHCP pool for both VLANs just in case the DHCP server is enabled on the device. (Optional)

Step 8 Go to **Smart port** tab, make sure Smart port is enabled.

Step 9 Make sure **IP Phone+Desktop** is checked under Device Detection.

Step 10 Go to **Smartport Type** settings and select Macro for IP Phone+Desktop.

Step 11 Click on **Edit**. Make sure Macro Type is selected as **Built-in Macro**.

Step 12 Change **Macro Parameters**.

- Change the **Parameter2** value to the value of Data VLAN ID (in this case 2 as data VLAN is 2).
- Parameter3 value will automatically show 5 in case you see the operational voice VLAN as 5 under Auto voice VLAN settings.

Step 13 Save the running configuration to start up configuration.

Delete a Voice VLAN



Note If you run into an instance where you are not able to delete the voice VLAN and getting an error message: "**VLAN xxx cannot be deleted because it is used as the agreed Voice VLAN**", this is because of a behavior of the **Voice VLAN**. By default, our switches are configured with "**triggered auto voice VLAN**" option set to **enable** on any firmware **2.5.5.x** and lower. Once the switch receives the VSDP packets from other switch or CDP packets from UC router, the voice VLAN is automatically enabled.

If you want to delete the **Voice VLAN** for one reason or the other, you will need to follow a sequence of steps for it to succeed. Via the GUI, here what you can do:

Procedure

Step 1 Select **VLAN Management** > **Voice VLAN** > **Properties**, and set **Dynamic Voice VLAN** to **Disable**.

Step 2 In **VLAN Management** > **Voice VLAN** > **Properties**, and set **Voice VLAN Id** to 1 (this is to remove the Voice ID that is being used in the setup and set the value to default 1).

Step 3 Return back to **VLAN Management** > **VLAN Settings** and delete the VLAN that was being used as the **Voice VLAN**

Note
However, that if you re-enable **Dynamic Voice VLAN**, the VLAN you removed will automatically be re-created and set as **Voice VLAN**.

Troubleshooting Link Flapping

This troubleshooting tip will help to resolve link flapping issues in the Cisco Business switches.



Note Whenever link flapping occurs between switches that are either stacked or there is an uplink with the another switch; follow the steps below to get the issue resolved.

Procedure

Step 1 Make sure that both switches are upgraded to the latest firmware version and that both switches are running the same firmware.

Step 2 Disable the Discovery-Bonjour Protocol by clicking **Administration > Discovery-Bonjour > Disable**.

Step 3 Disable **EEE** (Energy Efficient Ethernet) on both the switches, by clicking **Port Management**>**Green ethernet**>**Properties**> **802.3 Energy Efficient Ethernet (EEE)**> **Disable**.

Step 4 Enable **Link Flap Prevention** in both the switches by clicking on **Port Management**>**Error Recovery.**Next, check **Enable** in **Link Flap Prevention** to enable.

Step 5 Disable **LLDP** if issue persists after the Steps 1 to 4. Click **Administration > Discovery-LLDP Properties > LLDP Status > Disable**).

If Steps 1 to 5 do not help to resolve the link flapping, then remove all port on the port used for uplink/stacking.

Important: In case stacking is configured then you must remove the ports from stacking and configure them again.

Identifying Link Flapping

A link flap occurs when a physical interface on the switch continually goes up and down, three or more times a second for duration of at least ten seconds. The common cause is usually related to bad, unsupported, or non-standard cable or Small Form-Factor Pluggable (SFP) or related to other link synchronization issues. The cause for link flapping can be intermittent or permanent.

Since link flapping tends to be a physical interference, this section explains the steps that can be taken to diagnose and prevent it.

Procedure

Step 1 Try changing cables and monitor. If the issue persists, proceed to Step 2

Step 2 Go to **Status and Statistics > Diagnostics > Copper Test**.

Step 3 Select the Port from the drop-down menu and click on **Copper Test**.

Step 4 A warning will appear. Be aware that the port will be shut down for a short period of time. Choose **OK**.

Step 5 The *Test Results* will be displayed. If it says OK, it is most likely not the cable. If the results are not OK, change the cable and repeat the copper test to confirm that it is not the cable.

Analyzing your Topology

To confirm it is a physical problem and not a configuration issue on the switch, you need to analyze the devices connected to your switch. Check the following:

a. What devices are connected to the switch?

- Analyze each device connected to the switch. Have you experienced any issues with those devices?

b. Which ports are causing the problem and which devices are connected to those ports?

- Test the ports by connecting other devices and verifying if the problem continues.
- See if the device is causing issues on another port.

c. Is it the port or the device?

- Determining whether it is the port, or the device determines how to continue the troubleshooting process.
- If it is the device, you may have to contact support management for that device.
- If you have determined it is the port, it is time to check whether the issue is related to configuration or a physical one.

Configure Link Flap Prevention

Link flap prevention minimizes the disruption to switch and network operations in a link flap situation. It stabilizes the network topology by automatically setting the ports that experience excessive link flap events to *err-disable*. This mechanism also provides time to debug and locate the root cause for the flapping. A Syslog message or Simple Network Management Protocol (SNMP) trap is sent to alert regarding link flap and port shutdown. The interface will become active again only if specifically enabled by you or your system administrator.

Procedure

Step 1 Log into your switch Web User Interface (UI).

Step 2 Change to **Advanced Mode**.

Step 3 Go to **Port Management > Port Settings**.

Step 4 Check the Enable box for *Link Flap Prevention*. Press **Apply**.

Step 5 Click on **Save** to save your configurations.

Spanning Tree Protocol

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- Root—A forwarding port elected for the spanning-tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root bridge in the spanning tree
- Backup—A blocked port in a loopback configuration

The switch that has all of its ports as the designated role or as the backup role is the root switch. The switch that has at least one of its ports in the designated role is called the designated switch.

STP provides a tree topology for any arrangement of switches and interconnecting links, by creating a unique path between end stations on a network, and thereby eliminating loops.

The device supports the following Spanning Tree Protocol versions:

- Classic STP- Provides a single path between any two end stations, avoiding and eliminating loops.
- Rapid STP (RSTP)- Detects network topologies to provide faster convergence of the spanning tree. This is most effective when the network topology is naturally tree-structured, and therefore faster convergence might be possible. RSTP is enabled by default.
- Multiple STP (MSTP)- MSTP is based on RSTP. It detects Layer 2 loops, and attempts to mitigate them by preventing the involved port from transmitting traffic. Since loops exist on a per-Layer 2-domain basis, a situation can occur when a port is blocked to eliminate a STP loop. Traffic will be forwarded to the port that is not blocked, and no traffic will be forwarded to the port that is blocked. This is not an efficient usage of bandwidth as the blocked port will always be unused. MSTP solves this problem by enabling several STP instances, so that it is possible to detect and mitigate loops separately in each instance. This enables a port to be blocked for one or more STP instances but non blocked for other STP instances. If different VLANs are associated with different STP instances, then their traffic will be relayed based on the STP port state of their associated MST instances. Better bandwidth utilization results.
- PVST+ /RPVST+ - (Rapid) Per VLAN Spanning Tree
  - PVST+ is a protocol that runs a separate instance of the 802.1Q STP standard protocol per VLAN
  - Rapid PVST+ is a protocol that runs a separate instance of the 802.1Q RSTP standard protocol per VLAN.

As part of PVST/RPVST+ operation, a separate PVST frame is sent for each VLAN defined on a port. This enables maintaining state and topology per each VLAN

- SSTP- Cisco switches use special Shared Spanning Tree Protocol (SSTP) Bridge Protocol Data Units (BPDUs) to exchange PVST+ and rapid PVST+ spanning tree topology information. They transmit SSTP BPDUs to the Cisco shared spanning tree MAC address 01-00-0C-CC-CC-CD. These BPDUs have a format based on a proprietary enhancement of IEEE standard 802.1Q. On the native VLAN, these BPDUs are untagged. When a port is configured in trunk mode with multiple VLANs, then it transmits the SSTP BPDUs on that port tagged for those VLANs.

Interoperation Between Spanning Tree Protocols

There are two main aspects to the interoperation of IEEE standard MSTP (including RSTP and STP) with PVST+ (and rapid PVST+). The first involves forming a common spanning tree between switches and regions running MSTP and PVST+. The second involves tunneling PVST+ spanning trees across MSTP regions.

When a Cisco switch configured with PVST+ receives IEEE standard RSTP BPDUs on a port, it recognizes them, and sends two versions of BPDUs on the port: SSTP format BPDUs and IEEE standard STP BPDUs. Similarly, a switch configured with rapid PVST+ recognizes IEEE standard RSTP BPDUs, and on any port that receives RSTP BPDUs, it sends two versions of BPDUs: SSTP format and IEEE standard RSTP format BPDUs.

There are differences between the ways that MSTP and PVST+ map spanning tree instances to VLANs: we know that PVST+ creates a spanning tree instance for every VLAN, whereas MSTP maps one or more VLANs to each MST instance. At the point where a PVST+ region meets an MSTP region, the set of PVST+ instances does not generally match the set of MST instances. Therefore, the PVST+ region and the MSTP region need to communicate with each other on a single common spanning tree instance.

Interoperation between an MSTP region and a PVST+ region via the Common Spanning Tree is achieved as follows.

MST and PVST+ both offer loop-free layer two topologies but they each use a different approach:

- MST maps multiple VLANs to an instance, reducing the number of spanning-tree instances.
- PVST+ calculates an instance for each spanning-tree instance.

PVST+ sends BPDUs for each instance/VLAN so you could let MST process each BPDU separately with the instance that is configured for the VLAN.

When an MST region is connected to a PVST+ topology, MST simulates PVST+ with a PVST simulation mechanism. The MST region will send PVST+ BPDUs (one for each VLAN) on the interfaces that are connected to PVST+ switches. These BPDUs all carry the same information and advertise the same root bridge. The interfaces that connect to the PVST+ topology are called boundary interfaces/ports. Since PVST+ switches now receive BPDUs for each VLAN from MST carrying the same information, they will all make the same decisions when selecting a root bridge, root port, etc.

It is easiest to configure your network so that the MST region is the root bridge in your network. If your PVST+ domain has the root bridge, then MST will use the same root port for all VLANs. If the root bridge is in your MST region, then you change the cost per VLAN on your PVST+ switches to use different root ports and use a bit of load balancing.

RSPAN Configuration

SPAN (Switch Port Analyzer), also known as port mirroring or port monitoring, selects network traffic for analysis by a network analyzer. A Cisco Switch Probe device or another Remote Monitoring (RMON) probe can be used as the network analyzer.

Port mirroring is a network device feature that sends a copy of network packets seen on a single device port, multiple device ports, or an entire Virtual Local Area Network (VLAN) to a network monitoring connection on another device port. This is commonly used for network appliances that require network traffic monitoring, such as intrusion detection systems. The data packets are processed by a network analyzer connected to the monitoring port for diagnosis, debugging, and performance monitoring.

The Remote Switch Port Analyzer (RSPAN) is a SPAN extension. RSPAN extends SPAN by allowing you to monitor multiple switches across your network and define the analyzer port on a remote switch. This means you'll be able to centralize your network capture devices.

RSPAN works by mirroring traffic from an RSPAN session's source ports onto a VLAN dedicated to the RSPAN session. This VLAN is then trunked to other switches, allowing RSPAN session traffic to traverse multiple switches. Traffic from the RSPAN session VLAN is simply mirrored out the destination port on the switch that contains the session's destination port.

The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The traffic from the source interfaces on the start device is copied to the RSPAN VLAN through a reflector port. This is a physical port that has to be set. It is used exclusively to build an RSPAN session. The "network" keyword is required when specifying the reflector port, and non-RSPAN traffic is allowed over the link.

The reflector port has these characteristics:

- It can be a physical port that is assigned to an EtherChannel group, even if the EtherChannel group is specified as a SPAN source. The port is removed from the group while it is configured as a reflector port.
- A port used as a reflector port cannot be a SPAN source or destination port, nor can a port be a reflector port for more than one session at a time.
- It is invisible to all VLANs.
- Spanning tree is automatically disabled on a reflector port.
- A reflector port receives copies of sent and received traffic for all monitored source ports.

RSPAN Traffic Flow

- Each RSPAN session's traffic is routed over a user-specified RSPAN VLAN that is dedicated to that RSPAN session in all participating switches.
- The traffic from the start device's source interfaces is copied to the RSPAN VLAN via a reflector port. This is a physical port that must be configured and requires a "network" keyword that allows other traffic over the link.
- This reflector port serves as a mechanism for copying packets to an RSPAN VLAN.
- RSPAN traffic is then routed through trunk ports on intermediate devices to the final switch's destination session.

- The RSPAN VLAN is monitored by the destination switch and copied to a destination port.

RSPAN Port Membership Rules

- On all switches — Membership in RSPAN VLAN can be tagged only.
- Start Switch
  - SPAN source interfaces are not permitted to be members of the RSPAN VLAN.
  - Reflector port cannot be a member of this VLAN.
- Intermediate Switch
  - It is recommended that RSPAN membership be removed from all ports that are not used to pass mirrored traffic.
  - An RSPAN VLAN typically has two ports.
- Final Switch
  - Mirrored traffic requires that the source ports be members of the RSPAN VLAN.
  - RSPAN membership should be removed from all other ports, including the destination interface.

Multicast

Multicast offers an efficient communication mechanism for sending messages to multiple recipients in separate locations. It is also capable of supporting many-to-many and many-to-one communication.

Multicast applications use User Datagram Protocol (UDP) on IP. Messages are sent by a source (called the sender) and will send messages (termed as a stream) even if there is not another device on the network interested in receiving that information. Receivers, on the other hand, must subscribe to a particular multicast stream in order to inform the network to forward those messages.

IP multicasting is an efficient way to use network resources, especially for bandwidth-intensive services such as audio and video. IP multicast routing enables a host (source) to send packets to a group of hosts (receivers) anywhere within the IP network by using a special form of IP address called the IP multicast group address. The sending host inserts the multicast group address into the IP destination address field of the packet, and IP multicast routers and multilayer switches forward incoming IP multicast packets out all interfaces that lead to members of the multicast group. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message

Default IP Multicast Routing Configuration

This table displays the default IP multicast routing configuration.

Table 5: Default IP Multicast Routing Configuration

Feature	Default Settings
Multicast routing	Disabled on all interfaces.

Feature	Default Settings
Candidate BSRs	Disabled.
Candidate RPs	Disabled.
Shortest-path tree threshold rate	0 kb/s.

Understanding IGMP

Internet Group Management Protocol (IGMP) is a protocol designed for multicast purposes. With IGMP, you can establish group memberships between different users within a network. IGMP is mainly used for multimedia streaming, such as video-chat, between different users in a network. Snooping is the term used when a third party in a communication listens or observes the current connection data traffic. Therefore, IGMP Snooping is a process that listens specifically to multicast traffic. You can enable IGMP Snooping to forward multicast traffic to only already registered multicast clients on specific ports of the switch. This way, the multicast frames are only forwarded to a specific multicast client within a VLAN instead of to all the users in that VLAN.

Multicast is the network layer technique used to transmit data packets from one host to selected hosts in the network. At the lower layer, the switch broadcasts the multicast traffic on all ports, even if only one host needs to receive it. Internet Group Management Protocol (IGMP) snooping is used to forward Internet Protocol version 4 (IPv4) multicast traffic to the desired host. On the other hand, Multicast Listener Discovery (MLD) snooping is used to forward Internet Protocol version 6 (IPv6) multicast traffic to the desired hosts.

When IGMP is enabled, it detects the IGMP messages exchanged between the IPv4 router and the multicast hosts attached to the interfaces. It then maintains a table that restricts IPv4 multicast traffic and forwards them dynamically to the parts that need to receive them.

The following configurations are prerequisites for configuring IGMP.

1. Configure Virtual Local Area Network (VLAN).
2. Enable Bridge Multicast Filtering.

When MLD is enabled, it detects the MLD messages exchanged between the IPv6 router and the multicast hosts attached to the interfaces. It then maintains a table that restricts IPv6 multicast traffic and forwards them dynamically to the ports that need to receive them.

IGMP_MLD Proxy

IGMP/MLD Proxy is a simple IP Multicast protocol. Using IGMP/MLD Proxy to replicate Multicast traffic on devices like edge boxes can make the design and installation of these devices a lot easier. It decreases not just the cost of the devices, but also the operational overhead, by not supporting more advanced Multicast routing protocols like Protocol Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP).

Another benefit is that it makes proxy devices independent of the core network routers' Multicast routing protocol. As a result, proxy devices are simple to set up in any Multicast network.

IGMP/MLD Proxy Tree

The IGMP/MLD Proxy operates in a simple tree topology in which a robust Multicast routing protocol is not required (for example, PIM). It is sufficient to utilize a simple IPM Routing system based on learning group membership and proxy group membership information and forwarding Multicast packets based on that information. Each proxy device must be manually setup by identifying upstream and downstream interfaces.

In addition, the proxying tree topology's IP addressing scheme should be adjusted such that a proxy device can win the IGMP/MLD Querier election and forward Multicast traffic. Within the tree, there should be no other Multicast routers except the proxy devices, and the root of the tree should be connected to a larger multicast structure.

A proxy device that uses IGMP/MLD forwarding has a single upstream interface and one or more downstream interfaces. These designations are explicitly configured; no protocol exists to determine the type of each interface. On its downstream interfaces, a proxy device performs the router portion of IGMP/MLD, and on its upstream interface, it performs the host portion of IGMP/MLD.

Forwarding Rules and Querier

The following rules are applied.

- A Multicast packet received on the upstream interface is forwarded on all downstream interfaces requesting the packet only if the proxy device is the querier on the interfaces.
- A proxy device drops Multicast packets received on a downstream interface if it is not the querier on the interface.
- A Multicast packet received on a downstream interface on which the proxy device is the querier is forwarded on the upstream interface and on all downstream interfaces requesting the packet only if the proxy device is the querier on the interfaces.

Configuring IGMP Snooping for Multicast Forwarding

For IGMP to work, an IGMP querier is required. While a Multicast router is more appropriate in Multicast handling, the Cisco Small Business Switches can fulfill part of that role as long as the configuration is done properly.

Because of IGMP snooping is linked to the VLAN to which multicast traffic is flowing, one can think of having a multicast sever located in one VLAN while the subscriber is located in a different VLAN.

In this setup, 2 VLANs will be used. One VLAN where multicast traffic will take place, VLAN 115, and the second VLAN is the default; in our case, it is VLAN 1.

Procedure

Step 1 For the VLAN assignment, Switch B, the non-querier switch is uplinked to SW A, the querier through their ports 3. Both ports will be set as Trunk 1U, 115T (VLAN 1 untagged, VLAN 115 tagged).

a) Port 1 of switch A will have the Multicast server connected to it, VLAN 115U, Access
b) Port 2 of switch A will have the subscriber connected to it, VLAN 115U, Access
c) Port 1 of switch B will have the subscriber connected to it, VLAN 115U, Access
d) Port 2 of switch B will have the subscriber connected to it, VLAN 115U, Access
e) Port 10 of Switch A will have the router connected to it, VLAN 1U, 115T, Trunk

Step 2 The port on the router to which the switch is connected to should be a trunk port VLAN 1U, 115T. Make sure corresponding IP addresses, and DHPC settings are set as appropriate.

Step 3 Go to the main configuration page for **Multicast** > **IGMP Snooping** on the switch. The location of this page will be different based on the switch model.

Step 4 Check Enable for the following:

- IGMP Snooping Status
- IGMP Querier Status

Step 5 Next, select VLAN 115 and click **Edit**.

Step 6 Check **Enable** to enable IGMP Snooping Status.

Step 7 Check **MRouter Ports Auto Learn** to enable. This option is for the switch to automatically learn where the querier (Multicast Router) is located. Therefore, do no check this option if the switch will be acting as the querier.

Step 8 Check **Immediate Leave** to enable. This option can be enabled or disabled without fear of side effects to IGMP Snooping functionality. When enabled, it is meant to reduce the time it takes to block unnecessary IGMP traffic sent to a device port.

Step 9 Leave the Last Member Query Counter to its default setting and close the window to proceed to the next step.

Step 10 Go back to the main configuration page for **Multicast** > **IGMP Snooping** on the switch. The location of this page will be different based on the switch model.

Step 11 Check **IGMP Querier Status** to enable. Only enable this option if this switch will be acting as a querier, otherwise, leave it alone. In our case, only one querier is being set.

Step 12 Next, select VLAN 115 and click **Edit**.

Step 13 Check **IGMP Querier Status** to enable the switch to act as a querier. Please do so only if this switch is intended to act as a querier. In most setup, only one querier is needed.

Step 14 Check **IGMP Querier Election**. This option can be used to manage a situation where more than 1 querier in the VLAN is being used and that IGMP Querier Status is globally enabled on the second querier.

Step 15 Select the IGM Querier version, (version 2 or version 3). Most of the time it will be version 2 since selecting version 3 is used when there are switches and /or routers in the VLAN that perform source-specific IP Multicast forwarding.

Step 16 Select “User Defined” for “Querier Source IP address” and select the IP address of the switch that is acting as the querier.

Step 17 Now that tweaks have been made on snooping page, we need to enable Bridge multicast Filtering to make the whole thing to work. Go to **Multicast > Properties** on the web UI of the switch.

Step 18 Check **Bridge Multicast Filtering Status** to enable the switch to handle multicast in concert with IGMP snooping. If this feature is not checked, which is the default, multicast traffic is seen across all the ports.

Step 19 Select VLAN 115 or any specific VLAN. Select the “Forwarding Method”; here we selected “**IP Group Address**” so that Multicast IP address is seen in “Multicast /IP Multicast Group Address” table instead of MAC addresses in “Multicast /MAC Group Address” table if “MAC Group Address” was chosen instead.

Step 20 By default, Multicast Router Port is set to **None**. No need to adjust anything here. On a non-querier switch, the uplink port to the querier device will be selected as Dynamic. To check on this, select VLAN 115, hit “go” and note port 3 is selected on Dynamic row. This is to indicate that switch B is a non-querier but has detected a querier on its uplink port.

Step 21 Click **Multicast > Forward All** and make sure that it is set to **None**. It is normally set to "None" by default. This also applies to the querier switch.

Step 22 Click **Multicast > Unregistered Multicast**. The default setting is set to Forwarding all, meaning, all multicast traffic, registered or unregistered are forwarded. If you do not want unregistered traffic to be forwarded, then set it to “Filtering” which is recommended, and only keep the “Forwarding” setting selected only on ports where the Multicast server machines are connected.

Step 23 Test to see if it works. Using VLC as the video streaming program and the video subscriber client, connect the devices are shown in the diagram. From the VLC server, start streaming video and start the client to subscribe to those streams. The results:

Using VLC as the video streaming program and the video subscriber client, connect the devices are shown in the diagram. From the VLC server, start streaming video and start the client to subscribe to those streams. The results:

- Verify that the Multicast IP address is properly populated on Multicast /IP Multicast Group Address in VLAN 115. This is an indication that the client has successfully subscribed to the Video Streams
- In a setup of more than one switch, verify that the switch that is not acting as the querier has successfully identified the querier. On a non-querier switch, the uplink port to the querier device will be selected as Dynamic. To check on this, select VLAN 115, hit go and note port 3 is selected on Dynamic row. This is to indicate that this SW B is a non-querier but has detected a querier on its uplink port.

Step 24 By default, multicast traffic is set on all ports on the switch until Multicast Bridge Filtering is enabled. If multicast traffic is emanated from VLAN x while subscribers are on VLAN y, the above configuration will not work. The use of Multicast TV can be used to accommodate this special configuration.

802_1x Overview

802.1x authentication restricts unauthorized clients from connecting to a LAN through publicity-accessible ports. 802.1x authentication is a client-server model. In this model, network devices have the following specific roles.

- Client or supplicant
- Authenticator
- Authentication server

A network device can be either a client/supplicant, authenticator or both per port.

Client or Supplicant

A client or supplicant is a network device that requests access to the LAN. The client is connected to an authenticator.

If the client uses the 802.1x protocol for authentication, it runs the supplicant part of the 802.1x protocol and the client part of the EAP protocol.

Authenticator

An authenticator is a network device that provides network services and to which supplicant ports are connected. The following authentication modes on ports are supported.

- Single-host—Supports port-based authentication with a single client per port.
- Multi-host—Supports port-based authentication with a multiple clients per port.
- Multi-sessions—Supports client-based authentication with a multiple clients per port.

The following authentication methods are supported:

- 802.1x-based—Supported in all authentication modes.
- MAC-based—Supported in all authentication modes.
- WEB-based—Supported only in multi-sessions modes.

In 802.1x-based authentication, the authenticator extracts the EAP messages from the 802.1x messages (EAPOL packets) and passes them to the authentication server, using the RADIUS protocol.

With MAC-based or web-based authentication, the authenticator itself executes the EAP client part of the software on behalf on the clients seeking network access.

Open Access

In an 802.1x environment, the Open (Monitoring) Access feature assists in distinguishing genuine authentication failures from failures caused by misconfiguration and/or a lack of resources. Open Access assists system administrators in understanding the configuration issues of hosts connecting to the network, monitors bad situations, and allows these issues to be resolved.

When Open Access is enabled on an interface, the switch treats all RADIUS server failures as successes and allows access to the network for stations connected to the interfaces regardless of authentication results. Open Access modifies the standard behavior of blocking traffic on an authentication-enabled port until authentication and authorization are completed successfully.

Authentication's default behavior is still to block all traffic except Extensible Authentication Protocol over LAN (EAPoL). Open Access, on the other hand, gives the administrator the option of allowing unrestricted access to all traffic even if authentication (802.1X-based, MAC-based, and/or WEB-based) is enabled.

When RADIUS accounting is enabled, you can log authentication attempts and gain visibility of who and what is connecting to your network with an audit trail.

Authenticator Overview

Port Administrative Authentication States

The port administrative state determines whether the client is granted access to the network.

The following values are available:

- force-authorized-Port authentication is disabled and the port transmits all traffic in accordance with its static configuration without requiring any authentication. The switch sends the 802.1x EAP-packet with the EAP success message inside when it receives the 802.1x EAPOL-start message. This is the default state.
- force-unauthorized-Port authentication is disabled and the port transmits all traffic via the guest VLAN and unauthenticated VLANs. The switch sends 802.1x EAP packets with EAP failure messages inside when it receives 802.1x EAPOL-Start messages.
- auto-Enables 802.1 x authentications in accordance with the configured port host mode and authentication methods configured on the port.

Port Host Modes

Ports can be placed in the following port host modes.

- Single-Host Mode- A port is authorized if there is an authorized client. Only one host can be authorized on a port. When a port is unauthorized and the guest VLAN is enabled, untagged traffic is remapped to the guest VLAN. Tagged traffic is dropped unless it belongs to the guest VLAN or to an unauthenticated VLAN. If a guest VLAN is not enabled on the port, only tagged traffic belonging to the unauthenticated VLANs is bridged.

  When a port is authorized, untagged and tagged traffic from the authorized host is bridged based on the static VLAN membership port configuration. Traffic from other hosts is dropped. A user can specify that untagged traffic from the authorized host will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. Tagged traffic is dropped unless it belongs to the RADIUS-assigned VLAN or the unauthenticated VLANs.

- Multi-Host Mode- A port is authorized if there is if there is at least one authorized client. When a port is unauthorized and a guest VLAN is enabled, untagged traffic is remapped to the guest VLAN. Tagged traffic is dropped unless it belongs to the guest VLAN or to an unauthenticated VLAN. If guest VLAN is not enabled on a port, only tagged traffic belonging to unauthenticated VLANs is bridged.

  When a port is authorized, untagged and tagged traffic from all hosts connected to the port is bridged, based on the static VLAN membership port configuration. You can specify that untagged traffic from the authorized port will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. Tagged traffic is dropped unless it belongs to the RADIUS-assigned VLAN or to the unauthenticated VLANs.

- Multi-Sessions Mode-Unlike the single-host and multi-host modes, a port in the multi-session mode does not have an authentication status. This status is assigned to each client connected to the port. Tagged traffic belonging to an unauthenticated VLAN is always bridged regardless of whether the host is authorized or not.

  Tagged and untagged traffic from unauthorized hosts not belonging to an unauthenticated VLAN is remapped to the guest VLAN if it is defined and enabled on the VLAN, or is dropped if the guest VLAN is not enabled on the port. You can specify that untagged traffic from the authorized port will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. Tagged traffic is dropped unless it belongs to the RADIUS-assigned VLAN or to the unauthenticated VLANs.

Multiple Authentication Methods

If more than one authentication method is enabled on the switch, the following hierarchy of authentication methods is applied:

- 802.1x Authentication: Highest
- WEB-Based Authentication
- MAC-Based Authentication: Lowest

Multiple methods can run at the same time. When one method finishes successfully, the client becomes authorized, the methods with lower priority are stopped and the methods with higher priority continue.

When one of authentication methods running simultaneously fails, the other methods continue.

When an authentication method finishes successfully for a client authenticated by an authentication method with a lower priority, the attributes of the new authentication method are applied. When the new method fails, the client is left authorized with the old method.

802.1x Based Authentication

The 802.1x-based authenticator is responsible for relaying transparent EAP messages between 802.1x supplicants and authentication servers. The EAP messages exchanged between supplicants and the authenticator are encapsulated in 802.1x messages, and the EAP messages exchanged between the authenticator and authentication servers are encapsulated in RADIUS messages.

MAC-Based Authentication

MAC-based authentication is an alternative to 802.1X authentication that allows network access to devices that lack the 802.1X supplicant capability (such as printers and IP phones). MAC-based authentication grants or denies network access based on the MAC address of the connecting device. In this case, the switch supports EAP MD5 functionality with the username and password being the client's MAC address, as shown below.

Web-Based Authentication

End-users who request access to a network via a switch are authenticated using WEB-based authentication. It allows clients who are directly connected to the switch to be authenticated using a captive-portal mechanism before being granted network access.

Web-based authentication is client-based authentication that is supported in both Layer 2 and Layer 3 in the multi-sessions mode. When this method of authentication is enabled for a port, each host must authenticate itself in order to access the network. So you can have both authenticated and unauthenticated hosts on an enabled port.

When web-based authentication is enabled on a port, the switch drops all traffic from unauthorized clients, with the exception of ARP, DHCP, and DNS packets. The switch allows these packets to be forwarded so that even unauthorized clients can obtain an IP address and resolve host or domain names.

Unauthorized clients' HTTP/HTTPS over IPv4 packets are routed to the switch's CPU. When an end-user requests network access, if Web-based authentication is enabled on the port, a login page appears before the requested page. The user must enter his username and password, which are validated by a RADIUS server via the EAP protocol. The user is notified if authentication is successful.

The user's session has now been authenticated. While the session is in use, it remains open. The session is terminated if it is not used within a specified time interval. The system administrator configures this time interval, which is known as Quiet Time. When a session expires, the username and password are lost, and the guest must re-enter them to start a new one.

Unauthenticated VLANs and the Guest VLAN

Unauthenticated VLANs and the guest VLAN provide access to services that do not require the supplicant devices or ports to be authenticated and authorized.

The guest VLAN is the VLAN that is assigned to an unauthorized client. You can configure the guest VLAN and one or more VLANs to be unauthenticated in the 802.1x Authentication properties.

An unauthenticated VLAN is a VLAN that allows access by both authorized and unauthorized devices or ports. An unauthenticated VLAN has the following characteristics:

- It must be a static VLAN, and cannot be the guest VLAN or the default VLAN.
- The member ports must be manually configured as tagged members.
- The member ports must be trunk and/or general ports. An access port cannot be member of an unauthenticated VLAN.

The guest VLAN, if configured, is a static VLAN with the following characteristics:

- It must be manually defined from an existing static VLAN.
- The guest VLAN cannot be used as the Voice VLAN or an unauthenticated VLAN.

Host Modes with Guest VLAN

The host modes work with guest VLAN in the following way:

- Single-Host and Multi-Host Mode-Untagged and tagged traffic from the guest VLAN arriving on an unauthorized port are bridged through the guest VLAN. All other traffic is rejected. The traffic from an unauthenticated VLAN is routed through the VLAN.
- Multi-Sessions Mode in Layer 2-Untagged and tagged traffic that does not belong to the unauthenticated VLANs and arrives from unauthorized clients is assigned to the guest VLAN using the TCAM rule and bridged through the guest VLAN. The tagged traffic from an unauthenticated VLAN is routed through the VLAN.

  This mode cannot be configured on the same interface with policy-based VLANs.
- Multi-Sessions Mode in Layer 3-The mode does not support the guest VLAN.

RADIUS VLAN Assignment or Dynamic VLAN Assignment

If this option is enabled on the Port Authentication page, the RADIUS server can assign a VLAN to an authorized client. This is known as RADIUS-Assigned VLAN or Dynamic VLAN Assignment (DVA). The term RADIUS Assigned VLAN is used throughout this guide.

When a port is in multi-session mode and RADIUS-Assigned VLAN is enabled, the device adds the port as an untagged member of the VLAN that the RADIUS server assigns during the authentication process. Untagged packets are classified as belonging to the assigned VLAN if they originate from authenticated and authorized devices or ports.



Note In multi-session mode, RADIUS VLAN assignment is only supported when the device is in Layer 2 system mode.

For a device to be authenticated and authorized at a DVA-enabled port:

- The RADIUS server must authenticate the device and assign it a VLAN dynamically. In the Port Authentication page, you can set the RADIUS VLAN Assignment field to static. This allows the host to be bridged based on static configuration.
- DVA must be supported by a RADIUS server with the RADIUS attributes tunnel-type (64) = VLAN (13), tunnel-media-type (65) = 802 (6), and tunnel-privategroup-id = a VLAN ID.

When the RADIUS-Assigned VLAN feature is enabled, the host modes behave as follows:

- Single-Host and Multi-Host Mode- Untagged traffic and tagged traffic belonging to the RADIUS-assigned VLAN are bridged via this VLAN. All other traffic not belonging to unauthenticated VLANs is discarded

- Full Multi-Sessions Mode-Untagged traffic and tagged traffic not belonging to the unauthenticated VLANs arriving from the client are assigned to the RADIUS-assigned VLAN using TCAM rules and are bridged via the VLAN.
- Multi-Sessions Mode in Layer 3 System Mode

This mode does not support RADIUS-assigned VLAN.

The following table describes guest VLAN and RADIUS□VLAN assignment support depending on authentication method and port mode.

Table 6: VLAN and RADIUS-VLAN Assignment

Authentication Method	Single-host	Multi-host	Multi-sessions	
			Device in L3	Device in L2
802.1x	†	†	N/S	†
MAC	†	†	N/S	†
WEB	N/S	N/S	N/S	N/S

Legend

†- The port mode supports the guest VLAN and RADIUS-VLAN assignment

N/S-The port mode does not support the authentication method.

Violation Mode

In single-host mode you can configure the action to be taken when an unauthorized host on authorized port attempts to access the interface. This is done in the Host and Session Authentication page.

The following options are available:

- restrict-When a station attempts to access the interface with a MAC address other than the supplicant MAC address, a trap is generated. The shortest time between traps is one second. These frames are forwarded, but their source addresses remain unknown.
- protect-Frames with source addresses other than the supplicant address should be discarded.
- shutdown-Reject frames with source addresses other than the supplicant address and close the port.

The device can also be configured to send SNMP traps with a configurable minimum time between consecutive traps. Traps are disabled if seconds = 0. If no minimum time is specified, the restrict mode defaults to 1 second and the other modes to 0.

Quiet Period

Following a failed authentication exchange, the port (single-host or multi-host modes) or the client (multi-sessions mode) cannot attempt authentication during the Quiet period. The period is defined per port in single-host or multi-host mode, and it is defined per client in multi-sessions mode. The switch does not accept or initiate authentication requests during the quiet period.

Only 802.1x-based and Web-based authentications are subject to the period. You can also specify the number of login attempts allowed before the quiet period begins. A value of 0 indicates that the number of login

attempts is unlimited. The Port Authentication page allows you to configure the duration of the quiet period as well as the maximum number of login attempts.

Mode Behavior

The following table describes how authenticated and non-authenticated traffic is handled in various situations.

	Unauthenticated Traffic				**Authenticated Traffic**		
	With Guest VLAN		**Without Guest VLAN**		**With Radius VLAN**		**Without Radius**
	Untagged	**Tagged**	**Untagged**	**Tagged**	**Untagged**	**Tagged**	**Untagged**
Single-host	Frames are re-mapped to the guest VLAN	Frames are dropped unless they belong to the guest VLAN or to the unauthenticated VLANs	Frames are dropped	Frames are dropped unless they belong to the unauthenticated VLANs	Frames are re-mapped to the RADIUS assigned VLAN	Frames are dropped unless they belong to the RADIUS VLAN or to the unauthenticated VLANs	Frames are bridged based on the static VLAN configuration
Multi-host	Frames are re-mapped to the guest VLAN	Frames are dropped unless they belongs to the guest VLAN or to the unauthenticated VLANs	Frames are dropped	Frames are dropped unless they belongs to the unauthenticated VLANs	Frames are re-mapped to the Radius assigned VLAN	Frames are dropped unless they belongs to the Radius VLAN or to the unauthenticated VLANs	Frames are bridged based on the static VLAN configuration
Lite multi-sessions	N/S	N/S	Frames are dropped	Frames are dropped unless they belongs to the unauthenticated VLANs	N/S	N/S	Frames are bridged based on the static VLAN configuration

	Unauthenticated Traffic				Authenticated Traffic		
	With Guest VLAN		Without Guest VLAN		With Radius VLAN		Without Radi
	Untagged	Tagged	Untagged	Tagged	Untagged	Tagged	Untagged
Full multi-sessions	Frames are re-mapped to the guest VLAN	Frames are re-mapped to the guest VLAN unless they belongs to the unauthenticated VLANs	Frames are dropped	Frames are dropped unless they belongs to the unauthenticated VLANs	Frames are re-mapped to the RADIUS assigned VLAN	Frames are re-mapped to the Radius VLAN unless they belongs to the unauthenticated VLANs	Frames are bridged based the static VL configuration

DHCPv4 Types and Interactions

DHCPv4 Snooping

DHCP snooping is a security feature that prevents false DHCP response packets from being received and logs DHCP addresses. This is accomplished by classifying ports on the device as trusted or untrusted.

A trustworthy port is one that is allowed to assign DHCP addresses and is connected to a DHCP server. The device allows DHCP messages received on trustworthy ports to pass through. A port that is not allowed to assign DHCP addresses is known as an untrusted port. Until you declare a port trusted, it is regarded untrusted by default.

DHCPv4 Relay

DHCP Relay relays DHCP packets to the DHCP server.

DHCPv4 in Layer 2 and Layer 3

The device relays DHCP messages received from VLANs that have DHCP Relay enabled in Layer 2 system mode. The device can also transmit DHCP signals received from VLANs that do not have IP addresses in Layer 3 system mode. Option 82 is automatically inserted whenever DHCP Relay is enabled on a VLAN without an IP address. This insertion takes place on a single VLAN and has no effect on the global administrative state of Option 82.

Transparent DHCP Relay

For Transparent DHCP Relay where an external DHCP relay agent is being used,do the following:

- Enable DHCP Snooping.
- Enable Option 82 insertion.
- Disable DHCP Relay.

For regular DHCP Relay:

- Enable DHCP Relay.
- No need to enable Option 82 insertion.

Option 82

Option 82 (DHCP Relay Agent Information Option) sends port and agent information to a central DHCP server, identifying the physical location of an allocated IP address on the network.

Option 82's main objective is to aid the DHCP server in determining the optimum IP subnet (network pool) from which to receive an IP address.

On the device, the following Option 82 settings are available:

- DHCP Insertion- Add Option 82 information to packets that do not have foreign Option 82 information.
- DHCP Pass through- Forward or reject DHCP packets that contain Option 82 information from untrusted ports. On trusted ports, DHCP packets containing Option 82 information are always forwarded.

The packet flow through the DHCP Relay, DHCP Snooping, and Option 82 modules is shown in the table below:

There are a variety of scenarios that could occur:

- Both the DHCP client and the DHCP server are on the same VLAN. A typical bridge passes the DHCP messages between the DHCP client and the DHCP server in this scenario.
- Both the DHCP client and the DHCP server are on different VLANs. Only DHCP Relay can and does broadcast DHCP messages between the DHCP client and the DHCP server in this case. Regular routers send unicast DHCP packets, therefore if DHCP Relay is enabled on a VLAN without an IP address or if the device is not a router (Layer 2), an external router is required.

DHCP Relay and only DHCP Relay relays DHCP messages to a DHCP server.

Interactions Between DHCPv4 Snooping, DHCPv4 Relay and Option 82

The tables below describe how the device behaves when various combinations of DHCP Snooping, DHCP Relay, and Option 82 are used. When DHCP Snooping is disabled and DHCP Relay is enabled, the following describes how DHCP request packets are handled.

	DHCP Relay VLAN with IP Address		**DHCP Relay VLAN without IP Address**	
	Packet arrives without Option 82	Packet arrives with Option 82	Packet arrives without Option 82	Packet arrives with Option 82
Option 82 Insertion Disabled	Packet is sent without Option 82	Packet is sent with the original Option 82	Relay – inserts Option 82 Bridge – no Option 82 is inserted	Relay – discards the packet Bridge – Packet is sent with the original Option 82

	DHCP Relay VLAN with IP Address		DHCP Relay VLAN without IP Address	
Option 82 Insertion Enabled	Relay – is sent with Option 82 Bridge – no Option 82 is sent	Packet is sent with the original Option 82	Relay – is sent with Option 82 Bridge – no Option 82 is sent	Relay – discards the packet Bridge – Packet is sent with the original Option 82

When both DHCP Snooping and DHCP Relay are enabled, the following is how DHCP request packets are handled:

	DHCP Relay VLAN with IP Address		DHCP Relay VLAN without IP Address	
	Packet arrives without Option 82	Packet arrives with Option 82	Packet arrives without Option 82	Packet arrives with Option 82
Option 82 Insertion Disabled	Packet is sent without Option 82	Packet is sent with the original Option 82	Relay – inserts Option 82 Bridge – no Option 82 is inserted	Relay – discards the packet Bridge – Packet is sent with the original Option 82
Option 82 Insertion Enabled	Relay – is sent with Option 82 Bridge – Option 82 is added (if port is trusted, behaves as if DHCP Snooping is not enabled)	Packet is sent with the original Option 82	Relay – is sent with Option 82 Bridge – Option 82 is added (if port is trusted, behaves as if DHCP Snooping is not enabled)	Relay – discards the packet Bridge – Packet is sent with the original Option 82

The following describes how DHCP Reply packets are handled when DHCP Snooping is disabled

	DHCP Relay VLAN with IP Address		DHCP Relay VLAN without IP Address	
	Packet arrives without Option 82	Packet arrives with Option 82	Packet arrives without Option 82	Packet arrives with Option 82

	DHCP Relay VLAN with IP Address		DHCP Relay VLAN without IP Address	
Option 82 Insertion Disabled	Packet is sent without Option 82	Packet is sent with the original Option 82	Relay –discards Option 82 Bridge – Packet is sent without Option 82	Relay – 1. If reply originates in device, packet is sent without Option 82 2. If reply does not originate in device, packet is discarded. Bridge – Packet is sent with the original Option 82
Option 82 Insertion Enabled	Packet is sent without Option 82	Relay – packet is sent without Option 82 Bridge – Packet is sent with Option 82	Relay –discards Option 82 Bridge – Packet is sent without Option 82	Relay – packet is sent without Option 82 Bridge – Packet is sent with Option 82

The following describes how DHCP reply packets are handled when both DHCP Snooping and DHCP Relay are enabled.

	DHCP Relay VLAN with IP Address		DHCP Relay VLAN without IP Address	
	Packet arrives without Option 82	Packet arrives with Option 82	Packet arrives without Option 82	Packet arrives with Option 82
Option 82 Insertion Disabled	Packet is sent without Option 82	Packet is sent with the original Option 82	Relay –discards Option 82 Bridge – Packet is sent without Option 82	Relay – 1. If reply originates in device, packet is sent without Option 82 2. If reply does not originate in device, packet is discarded. Bridge – Packet is sent with the original Option 82

	DHCP Relay VLAN with IP Address		DHCP Relay VLAN without IP Address	
Option 82 Insertion Enabled	Packet is sent without Option 82	Packet is sent without Option 82	Relay –discards Option 82 Bridge – Packet is sent without Option 82	Packet is sent without Option 82

IPv6 Management Interfaces

IPv6 (Internet Protocol Version 6) is a network-layer protocol for packet-switched internet operations. IPv6 was created to take the place of IPv4, the most widely used Internet protocol. Because the address size grows from 32 to 128 bits, IPv6 allows for more flexibility when allocating IP:-FE80::9C00:876A:130BFE80:0000:0000:0000:0000:9C00:876A:130B is an example of an abbreviated form in which a series of zeroes can be left out and replaced with '::'.

To connect with other IPv6 nodes over an IPv4-only network, IPv6 nodes require an intermediary mapping mechanism. This tunneling technology allows IPv6-only hosts to connect to IPv4 services, as well as isolated IPv6 hosts and networks to connect to an IPv6 node across IPv4 infrastructure.

An ISATAP or a manual mechanism is used for tunneling (see IPv6 Tunnel). The IPv4 network is treated as a virtual IPv6 local link, with mappings from each IPv4 address to a link local IPv6 address, via tunneling. The IPv6 Ethertype is used by the device to recognize IPv6 frames.

DoS Prevention

A Denial of Service (DoS) attack is an attempt by a hacker to make a device inaccessible to its users.

DoS attacks overload the device with external communication requests, preventing it from responding to legitimate traffic.

These attacks typically result in a device CPU overload.

Secure Core Technology (SCT)

The device employs SCT as one method of resisting DoS attacks. SCT on the device is enabled by default and cannot be disabled. In addition to end-user (TCP) traffic, the Cisco device handles management traffic, protocol traffic, and snooping traffic. SCT ensures that no matter how much total traffic is received, the device receives and processes management and protocol traffic. This is accomplished by limiting TCP traffic to the CPU.

There are no interactions with other features.

Types of DoS Attacks

The following types of packets or other strategies might be involved in a Denial of Service attack

- TCP SYN Packets—These packets frequently have an incorrect sender address. Each packet is treated as a connection request, causing the server to spawn a half-open connection by sending back a TCP/SYN-ACK packet (Acknowledgment) and waiting for a packet from the sender address (response to the ACK Packet). However, because the sender address is incorrect, the response is never received.

These half-open connections saturate the device's available connections, preventing it from responding to legitimate requests.

- TCP SYN-FIN Packets—To establish a new TCP connection, SYN packets are sent. TCP FIN packets are used to terminate a connection. A packet with both the SYN and the FIN flags set should never exist. As a result, these packets may indicate an attack on the device and should be blocked.
- Martian Addresses—Martian addresses are illegal from the point of view of the IP protocol.
- ICMP Attack—Sending malformed ICMP packets or a large number of ICMP packets to the victim, potentially causing a system crash.
- IP Fragmentation—The device receives mangled IP fragments with overlapping, over-sized payloads. Because of a bug in their TCP/IP fragmentation re-assembly code, this can cause various operating systems to crash.
- Stacheldraht Distribution—The attacker connects to handlers, which are compromised systems that issue commands to zombie agents, facilitating the DoS attack. The attacker compromises agents through the handlers. Using automated routines to exploit vulnerabilities in programs that accept remote connections and are running on the remote hosts under attack. Each handler has the ability to command up to a thousand agents.
- Invasor Trojan—A trojan that allows the attacker to download a zombie agent (or the trojan may contain one). Attackers can also gain access to systems by employing automated tools that exploit flaws in programs that listen for connections from remote hosts. This scenario primarily concerns the device when it acts as a web server.
- Back OrifaceTrojan—This is a trojan variant that uses Back Oriface software to install the trojan.

Defense Against DoS Attacks

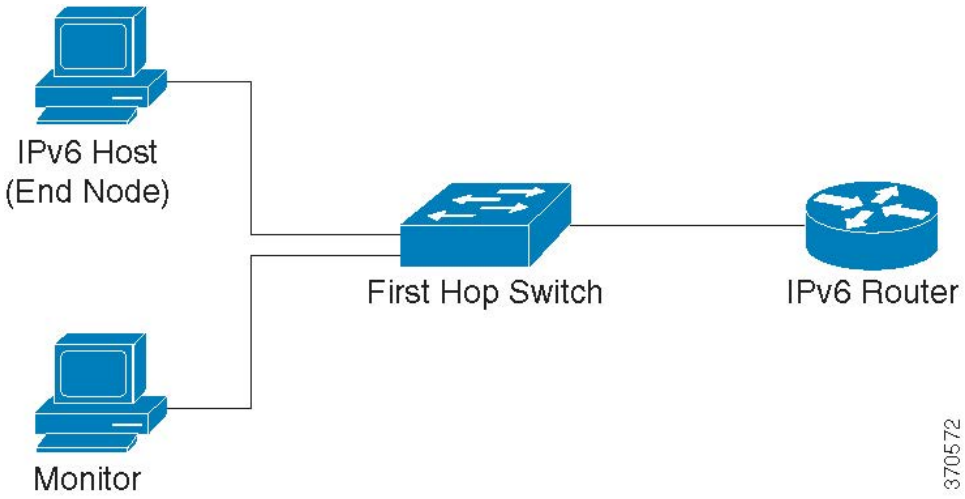
The Denial of Service (DoS) Prevention feature assists the system administrator in resisting such attacks in the following ways:

- Enable TCP SYN protection. If this feature is enabled, reports are issued when a SYN packet attack is identified, and the attacked port can be temporarily shut-down. A SYN attack is identified if the number of SYN packets per second exceeds a user-configured threshold.
- Block SYN-FIN packets.
- Block packets that contain reserved Martian addresses.
- Prevent TCP connections from a specific interface and rate limit the packets.
- Configure the blocking of certain ICMP packets.
- Discard fragmented IP packets from a specific interface. page)
- Deny attacks from Stacheldraht Distribution, Invasor Trojan, and Back Orifice Trojan.

IPv6 First Hop Security

IPv6 FHS is a suite of features designed to secure link operations in an IPv6-enabled network. It is based on the Neighbor Discovery Protocol and DHCPv6messages.

In this feature, a Layer 2 switch (as shown below) filters Neighbor Discovery Protocol messages, DHCPv6 messages and user data messages according to a number of different rules.



A separate and independent instance of IPv6 First Hop Security runs on each VLAN on which the feature is enabled.

Table 7: Abbreviations

Name	Description
CPA message	Certification Path Advertisement message
CPS message	Certification Path Solicitation message
DAD-NS message	Duplicate Address Detection Neighbor Solicitation message
FCFS-SAVI	First Come First Served- Source Address Validation Improvement
NA message	Neighbor Advertisement message
NDP	Neighbor Discovery Protocol
NS message	Neighbor Solicitation message
RA message	Router Advertisement message
RS message	Router Solicitation message
SAVI	Source Address Validation Improvement

IPv6 First Hop Security Components

IPv6 First Hop Security includes the following features:

- IPv6 First Hop Security Common
- RA Guard
- ND Inspection

- Neighbor Binding Integrity
- DHCPv6 Guard
- IPv6 Source Guard

These components can be enabled or disabled on VLANs.

There are two empty, pre-defined policies for each feature, with the names VLAN default and port default. The first is connected to each VLAN that is not attached to a user-defined policy, and the second is connected to each interface and VLAN that is not attached to a user-defined policy. The user cannot explicitly attach these policies.

IPv6 First Hop Security Pipe

If IPv6 First Hop Security is enabled on a VLAN, the switch traps the following messages:

- Router Advertisement (RA) messages
- Router Solicitation (RS) messages
- Neighbor Advertisement (NA) messages
- Neighbor Solicitation (NS) messages
- ICMPv6 Redirect messages
- Certification Path Advertisement (CPA) messages
- Certification Path Solicitation (CPS) messages
- DHCPv6 messages

Trapped RA, CPA, and ICMPv6 Redirect messages are routed to the RA Guard feature. RA Guard validates these messages, discards illegal messages, and forwards legal messages to the ND Inspection feature. ND Inspection validates these messages and discards illegal messages, while legal messages are routed to the IPv6 Source Guard feature.

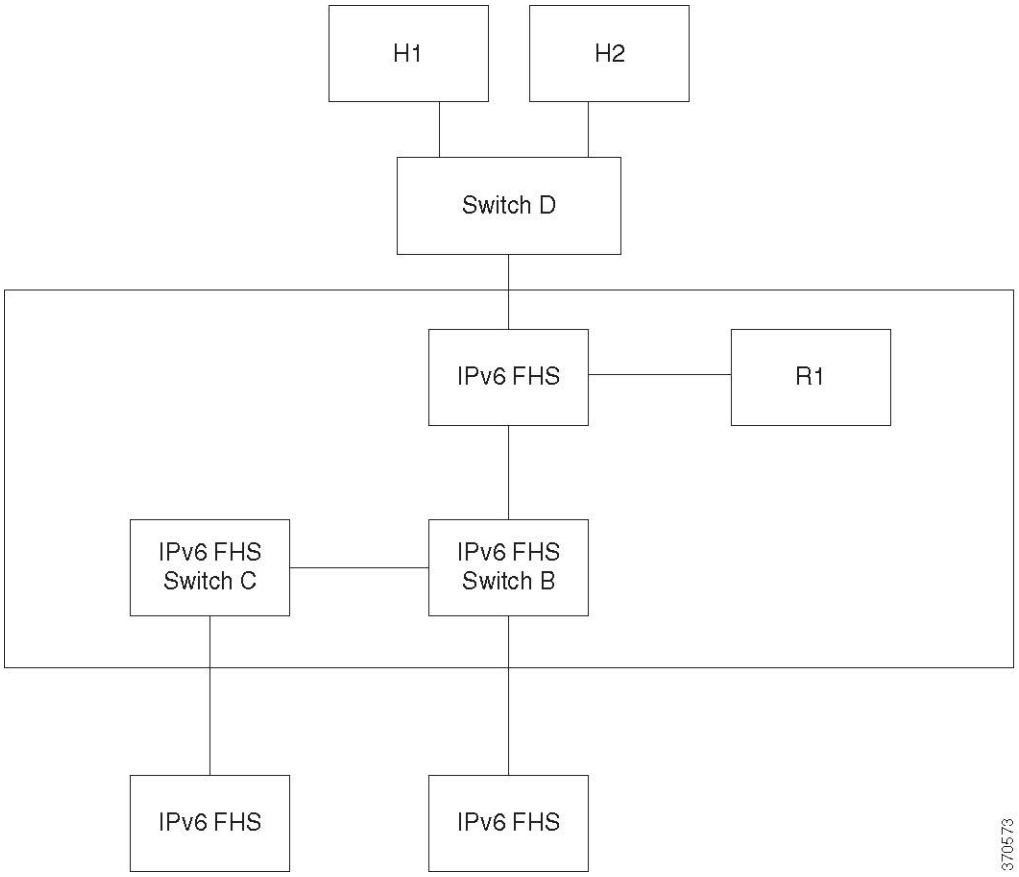
Trapped DHCPv6 messages are routed to the DHCPv6 Guard feature. DHCPv6 Guard validates these messages, discards illegal messages, and forwards legal messages to the IPv6 Source Guard feature.

Data messages that are being trapped are routed to the IPv6 Source Guard feature. Using the Neighbor Binding Table, IPv6 Source Guard validates received messages (trapped data messages, NDP messages from ND Inspection, and DHCPv6 messages from DHCPv6 Guard), drops illegal messages, and forwards legal messages. Neighbor Binding Integrity obtains neighbors from received messages (NDP and DHCPv6) and saves them in the Neighbor Binding table.

Static entries can also be manually added. After learning the addresses, the NBI feature forwards the frames. The ND Inspection feature also receives trapped RS,CPS,NS, and NA messages. ND Inspection validates these messages, discards illegal ones, and forwards legal ones to the IPv6 Source Guard feature.

IPv6 First Hop Security Perimeter

IPv6 First Hop Security switches can form a perimeter separating untrusted area from trusted area. All switches inside the perimeter support IPv6 First Hop Security, and hosts and routers inside this perimeter are trusted devices. For example, in the figure below, Switch B and Switch C are inner links inside the protected area.



The perimeter is specified by the device-role command in the Neighbor Binding policy configuration screen. Each IPv6 First Hop Security switch binds neighbors partitioned by the edge. Binding entries are distributed in this manner on IPv6 First Hop Security devices that form the perimeter. The IPv6 First Hop Security devices can then provide binding integrity to the inside of the perimeter without having to configure bindings for every address on each device.

Router Advertisement Guard

Router Advertisement (RA) Guard is the first FHS feature that treats trapped RA messages. RA Guard supports the following functions:

- Filtering of received RA, CPA, and ICMPv6 redirect messages. The RA Guard discards RA and CPA messages received on interfaces whose role are not router.
- Validation of received RA messages. The RA Guard validates RA messages using the filtering based on the RA Guard policy attached to the interface.

If a message does not pass verification, it is dropped. If the logging packet drop configuration on the FHS common component is enabled, a rate limited SYSLOG message is sent.

Neighbor Discovery Inspection

Neighbor Discovery (ND) Inspection supports the following functions:

- Validation of received Neighbor Discovery protocol messages
- Egress filtering

Message Validation

Based on an ND Inspection policy attached to the interface, ND Inspection validates the Neighbor Discovery protocol messages. On the ND Inspection Settings page, you can define this policy.

If a message fails the policy-defined verification, it is dropped and a rate-limited SYSLOG message is sent in its place.

Egress Filtering

ND Inspection blocks forwarding of RS and CPS messages on interfaces configured as host interfaces.

Neighbor Binding Integrity

Neighbor Binding (NB) Integrity establishes binding of neighbors. A separate, independent instance of NB Integrity runs on each VLAN on which the feature is enabled.

Learning Advertised IPv6 Prefixes

NB Integrity learns IPv6 prefixes advertised in RA messages and saves it in the Neighbor Prefix table. The prefixes are used for verification of assigned global IPv6 addresses. By default, this validation is disabled. When it is enabled, addresses are validated against the prefixes in the Neighbor Binding Settings page. Static prefixes used for the address validation can be added in the Neighbor Prefix Table page.

Validation of Global IPv6 Addresses

NB Integrity performs the following validations:

- If the target address in an NS or NA message is a global IPv6 address, it must belong to one of the prefixes defined in the RA Prefix table.
- A global IPv6 address provided by a DHCPv6 server must belong to one of the prefixes defined in the IPv6 Prefix List.

If a message does not pass this verification, it is dropped and a rate limited SYSLOG message is sent.

Neighbor Binding Table Overflow

When there is no free space to create a new entry, no entry is created and a SYSLOG message is sent.

Establishing Binding of Neighbors

An IPv6 First Hop Security switch can discover and record binding information by using the following methods:

- NBI-NDP Method: Learning IPv6 addresses from the snooped Neighbor Discovery Protocol messages
- NBI-DHCP method: By learning IPv6 addresses from the snooped DHCPv6 messages
- NBI-Manual Method: By manual configuration

An IPv6 address is bound to a link layer property of the host's network attachment. This property, called a "binding anchor" consists of the interface identifier (if Index) through which the host is connected to and the host’s MAC address.

IPv6 First Hop Security switch establishes binding only on perimeterical interfaces. Binding information is saved in the Neighbor Binding table

NBI-NDP Method

The NBI-NDP method used is based on the FCFS- SAVI method specified in RFC6620, with the following differences:

- Unlike FCFS-SAVI, which supports only binding for link local IPv6 addresses, NBI-NDP additionally supports binding global IPv6 addresses as well.
- NBI-NDP supports IPv6 address binding only for IPv6 addresses learned from NDP messages. Source address validation for data message is provided by IPv6 Source Address Guard.
- In NBI-NDP, proof of address ownership is based on the First-Come, First- Served principle. The first host that claims a given source address is the owner of that address until further notice. Since no host changes are acceptable, a way must be found to confirm address ownership without requiring a new protocol. For this reason, whenever an IPv6 address is first learned from an NDP message, the switch binds the address to the interface. Subsequent NDP messages containing this IPV6 address can be checked against the same binding anchor to confirm that the originator owns the source IP address.

  The exception to this rule occurs when an IPv6 host roams in the L2 domain or changes its MAC address. In this case, the host is still the owner of the IP address, but the associated binding anchor might have changed. To cope with this case, the defined NBI-NDP behavior implies verification of whether or not the host is still reachable by sending DAD-NS messages to the previous binding interface. If the host is no longer reachable at the previously-recorded binding anchor, NBI-NDP assumes that the new anchor is valid and changes the binding anchor. If the host is still reachable using the previously recorded binding anchor, the binding interface is not changed.

To reduce the size of the Neighbor Binding table, NBI-NDP establishes binding only on perimeterical interfaces (see IPv6 First Hop Security Perimeter) and distributes binding information through internal interfaces using NS and NA messages. Before creating an NBI-NDP local binding, the device sends a DAD-NS message querying for the address involved. If a host replies to that message with an NA message, the device that sent the DAD-NS message infers that a binding for that address exists in another device and does not create a local binding for it. If no NA message is received as a reply to the DAD-NS message, the local device infers that no binding for that address exists in other devices and creates the local binding for that address.

NBI-NDP supports a lifetime timer. A value of the timer is configurable in the Neighbor Binding Settings page. The timer is restarted each time that the bound IPv6 address is confirmed. If the timer expires, the device sends up to 2 DAD-NS messages with short intervals to validate the neighbor.

NBI-DHCP Method

The NBI-NDP method is based on the SAVI-DHCP method specified in the SAVI Solution for DHCP, draft-ietf-savi-dhcp-15, September 11, 2012.

Like NBI-NDP, NBI-DHCP provides perimeterical binding for scalability. The following difference between the NBI-DHCP and NBI-FCFS method exists: NBIDHCP follows the state announced in DHCPv6 messages, thus there is no need to distribute the state by NS/NA messages.

NB Integrity Policy

In the same way that other IPv6 First Hop Security features function, NB Integrity behavior on an interface is specified by an NB Integrity policy attached to an interface. These policies are configured in the Neighbor Binding Settings page

DHCPv6 Guard

DHCPv6 Guard treats the trapped DHCPv6 messages. DHCPv6 Guard supports the following functions:

- Filtering of received DHCPv6 messages. DHCP Guard discards DHCPv6 reply messages received on interfaces whose role is client. The interface role is configured in the DHCP Guard Settings page.
- Validation of received DHCPv6 messages. DHCPv6 Guard validates DHCPv6 messages that match the filtering based on the DHCPv6 Guard policy attached to the interface.

If a message does not pass verification, it is dropped. If the logging packet drop configuration on the FHS common component is enabled, a rate limited SYSLOG message is sent.

IPv6 Source Guard

If Neighbor Binding Integrity (NB Integrity) is enabled, IPv6 Source Guard validates the source IPv6 addresses of NDP and DHCPv6 messages, regardless of whether IPv6 Source Guard is enabled. If IPv6 Source Guard is enabled together with NB Integrity, IPv6 Source Guard configures the TCAM to specify which IPv6 data frames should be forwarded, dropped, or trapped to the CPU and validates the source IPv6 addresses of the trapped IPv6 data messages. If NB Integrity is not enabled, IPv6 Source Guard is not activated regardless of whether it is enabled or not.

If the TCAM does not have free room to add a new rule, the TCAM overflow counter is Incremented and a rate-limited SYSLOG message containing the interface identifier, host MAC address, and host IPv6 address is sent. IPv6 Source Guard validates the source addresses of all received IPv6 messages using the Neighbor Binding table except for the following messages that are passed without validation:

- RS messages, if the source IPv6 address equals the unspecified IPv6 address.
- NS messages, if the source IPv6 address equals the unspecified IPv6 address.
- NA messages, if the source IPv6 address equals the target address.

IPv6 Source Guard drops all other IPv6 messages whose source IPv6 address equals the unspecified IPv6 address. IPv6 Source Guard runs only on untrusted interfaces belonging to the perimeter.

IPv6 Source Guard drops an input IPv6 message if:

- The Neighbor Binding table does not contain the IPv6 address
- The Neighbor Binding table contains the IPv6 address, but it is bound to another interface.

IPv6 Source Guard initiates the Neighbor Recovery process by sending DAD_NS messages for the unknown source IPv6 addresses

-

Attack Protection

The section describes attack protection provided by IPv6 First Hop Security

Protection against IPv6 Router Spoofing

An IPv6 host can use the received RA messages for:

- IPv6 router discovery
- Stateless address configuration

A malicious host could send RA messages advertising itself as an IPv6 router and providing counterfeit prefixes for stateless address configuration. RA Guard provides protection against such attacks by configuring the interface role as a host interface for all interfaces where IPv6 routers cannot be connected.

Protection against IPv6 Address Resolution Spoofing

A malicious host could send NA messages advertising itself as an IPv6 Host having the given IPv6 address. NB Integrity provides protection against such attacks in the following ways:

- If the given IPv6 address is unknown, the Neighbor Solicitation (NS) message is forwarded only on inner interfaces.
- If the given IPv6 address is known, the NS message is forwarded only on the interface to which the IPv6 address is bound.
- A Neighbor Advertisement (NA) message is dropped if the target IPv6 address is bound with another interface.

Protection against IPv6 Duplication Address Detection Spoofing

An IPv6 host must perform Duplication Address Detection for each assigned IPv6 address by sending a special NS message (Duplicate Address Detection Neighbor Solicitation message (DAD_NS) message).

A malicious host could send reply to a DAD_NS message advertising itself as an IPv6 host having the given IPv6 address. NB Integrity provides protection against such attacks in the following ways:

- If the given IPv6 address is unknown, the DAD_NS message is forwarded only on inner interfaces
- If the given IPv6 address is known, the DAD_NS message is forwarded only on the interface where the IPv6 address is bound.
- An NA message is dropped if the target IPv6 address is bound with another interface.

Protection against DHCPv6 Server Spoofing

An IPv6 host can use the DHCPv6 protocol for:

- Stateless information configuration
- Stateless address configuration

Protection Against NBD Cache Spoofing

An IPv6 router supports the Neighbor Discovery Protocol (NDP) cache that maps the IPv6 address to the MAC address for the last hop routing. A malicious host could send IPv6 messages with a different destination IPv6 address for the last hop forwarding, causing overflow of the NBD cache.

An embedded mechanism in the NDP implementation limits the number of entries allowed in the INCOMPLETE state in the Neighbor Discovery cache. This provides protection against the table being flooded by hackers.

Secure Sensitive Data Management

Secure Sensitive Data (SSD) is an architecture that allows sensitive data on a device, such as passwords and keys, to be protected. Passwords, encryption, access control, and user authentication are used to create a secure approach for managing sensitive data at the institution.

The capability has been enhanced to safeguard configuration files, secure the configuration process, and facilitate SSD zero-touch auto configuration.

SSD secures sensitive data on a device, such as passwords and keys, by allowing and disallowing access to sensitive data encrypted and in plain text based on user credentials and SSD rules, and by preventing tampering with configuration files holding sensitive data.

Furthermore, SSD allows for the secure backup and sharing of configuration files containing sensitive information.

Users can select the level of protection they want for their sensitive data, ranging from no protection with sensitive data in plaintext to minimal protection with encryption based on the default pass phrase to higher protection with encryption based on user-defined pass phrase.

Only authenticated and authorized users are granted read privilege to sensitive data, and this is done in accordance with SSD regulations. Through the user authentication procedure, a device authenticates and authorizes management access to users. It is advised that the administrator protect the authentication process by using the local authentication database and/or secure the communication to the external authentication servers used in the user authentication process, regardless of whether SSD is utilized.

In summary, SSD uses SSD rules, SSD attributes, and user authentication to safeguard sensitive data on a device. And the device's SSD rules, SSD characteristics, and user authentication configurations are all critical data that SSD protects.

SSD Management

SSD management consists of a set of setup parameters that dictate how sensitive data is handled and secured. The SSD configuration parameters are sensitive information that is safeguarded by SSD.

All SSD configuration is done through the SSD pages, which are only accessible to those with the appropriate rights.

SSD Rules

The read privileges and default read mode assigned to a user session on a management channel are defined by SSD rules. The user and SSD management channel that an SSD rule belongs to give it a distinct identity. It's possible that distinct SSD rules exist for the same user but for different channels, and that different rules exist for the same channel but for different users.

Read permissions specify how sensitive data can be viewed: solely in encrypted form, exclusively in plaintext form, both encrypted and plaintext forms, or no authorization to access sensitive data at all. The SSD regulations are classified as sensitive data and are therefore safeguarded.

There are a total of 32 SSD rules that can be supported by a device. The SSD read permission of the SSD rule that best matches the user identity/credential and the type of management channel via which the user is/will access the sensitive data is granted to a user by a device.

A set of default SSD rules is included with every device. SSD rules can be added, deleted, and changed at any time by an administrator.

Default SSD Rules

The device has the following factory default rules:

Rule Key		Rule Action	
User	**Channel**	**Read Permission**	**Default Read Mode**
Level 15	Secure XML SNMP	Plaintext Only	Plaintext
Level 15	Secure	Both	Encrypted
Level 15	Insecure	Both	Encrypted
All	Insecure XML SNMP	Exclude	Exclude
All	Secure	Encrypted Only	Encrypted
All	Insecure	Encrypted Only	Encrypted

The default rules can be modified, but they cannot be deleted. If the SSD default rules have been changed, they can be restored.

Secure Shell

Secure Shell or SSH, is a network protocol that allows data to be sent securely between an SSH client (the device) and an SSH server.

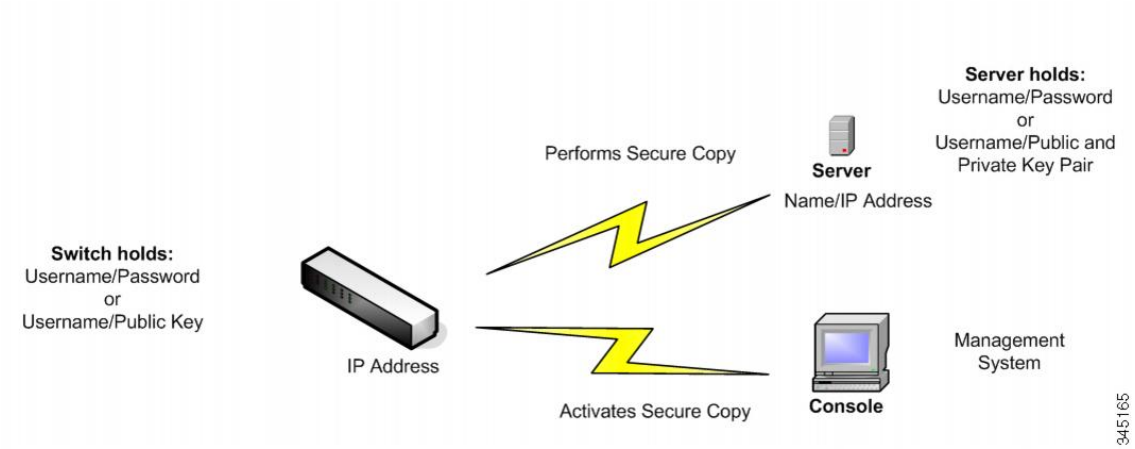
The SSH client aids in the management of a network consisting of one or more switches with various system files kept on a central SSH server. Secure Copy (SCP), an application that uses the SSH protocol to transfer configuration files over the network, ensures that sensitive data, such as username/password, is not intercepted. Secure Copy (SCP) is a method of transferring firmware, boot images, configuration files, language files, and log files from a central SCP server to a device in a secure manner.

With respect to SSH, the SCP running on the device is an SSH client application and the SCP server is a SSH server application.

The data transfer is secure when files are downloaded through TFTP or HTTP. When files are downloaded with SCP, the data is sent across a secure channel from the SCP server to the device. Authentication is required before this secure channel can be created, as it verifies that the user is authorized to conduct the activity. Although this article does not cover server operations, the user must submit authentication information on both the device and the SSH server.

The following diagram depicts a common network configuration that could benefit from the SCP functionality.

Typical Network Configuration



QoS

Quality of Service provides different priority to one or more types of traffic over other levels for different applications, data flows, or users to guarantee performance. QoS looks at many different variables that exist on an network in order to make decisions on how it is going to deal with the issue.

Problems that QoS Deals With

- Delay- less than ideal routes to the destination networks, and delays such as these can make some applications such as VoIP, fail.
    - Main reason to use QoS is real–time applications (RTA)
- Dropped Packets- Buffers are full and packets do not get processed in time so they are dropped. In a contention link QoS would prioritize traffic, so less important traffic would be dropped.
- Errors- Packets get corrupted for many reasons, but since we use TCP we will keep re-transmitting until we receave an ACK and that causes retransmissions and delays.
- Jitter- Packets may take multiple paths to a destination and may not be the most optimal path. This variation causes delays, which is called jitter. Jitter should be below 30 ms. Packet loss shouldn't be more than 1%
- Out of Order Delivery- Due to packets using varying paths to reach a destination, applications at the receiving end may take longer than expected to re-order the packets and cause delays and drops. QoS will ensure that applications with a required level of predictability will receive the needed bandwidth

QoS Mechanisms

- Classification- supported by a class-oriented QoS mechanism.
- Congestion Management- Used to prioritize the transmission of packets, with a queuing mechanism on each interface.
- Policing-Used to enforce a rate limit by dropping or marking down packets.

- Shaping- Used to enforce a rate limit by delaying packets, using buffers.

To configure general QoS parameters, perform the following:

Procedure

Step 1 Enable QoS by using the QoS Properties page to select the trust mode. Then enable QoS on ports by using the Interface Settings page.

Step 2 Assign each interface a default CoS or DSCP priority by using the QoS Properties page.

Step 3 Assign the schedule method (Strict Priority or WRR) and bandwidth allocation for WRR to the egress queues by using the Queue page.

Step 4 Designate an egress queue to each IP DSCP/TC value with the DSCP to Queue page. If the device is in DSCP trusted mode, incoming packets are put into the egress queues based on the their DSCP/TC value.

Step 5 Designate an egress queue to each CoS/802.1p priority. If the device is in CoS/802.1 trusted mode, all incoming packets are put into the designated egress queues according to the CoS/802.1p priority in the packets. This is done by using the CoS/802.1p to Queue page.

Step 6 Enter bandwidth and rate limits in the following pages:

a) Set egress shaping per queue by using the Egress Shaping Per Queue page.

b) Set ingress rate limit and egress shaping rate per port by using the Bandwidth page.

QoS Features and Components

The QoS feature is used to optimize network performance.

QoS provides the following:

- Classification of incoming traffic to traffic classes, based on attributes, including:
  - Device Configuration
  - Ingress interface
  - Packet content
  - Combination of these attributes

QoS includes the following:

- Traffic Classification—Classifies each incoming packet as belonging to a specific traffic flow, based on the packet contents and/or the port. The classification is done by ACL (Access Control List), and only traffic that meets the ACL criteria is subject to CoS or QoS classification.
- Assignment to Software Queues—Assigns incoming packets to forwarding queues. Packets are sent to a particular queue for handling as a function of the traffic class to which they belong.
- Other Traffic Class-Handling Attribute—Applies QoS mechanisms to various classes, including bandwidth management.

QoS Modes

The QoS mode that is selected applies to all interfaces in the system.

- Basic Mode—Class of Service (CoS).

  All traffic of the same class receives the same treatment, which is the single QoS action of determining the egress queue on the egress port, based on the indicated QoS value in the incoming frame. This can be the VLAN Priority Tag (VPT) 802.1p value in Layer 2 and the Differentiated Service Code Point (DSCP) value for IPv4 or Traffic Class (TC) value for IPv6 in Layer 3. When operating in Basic Mode, the device trusts this external assigned QoS value. The external assigned QoS value of a packet determines its traffic class and QoS.

- Advanced Mode—Per-flow Quality of Service (QoS).

  In advanced mode, a per flow QoS consists of a class map and/or a policer:

  - A class map defines the kind of traffic in a flow, and contains one or more ACLs. Packets that match the ACLs belong to the flow.
  - A policer applies the configured QoS to a flow. The QoS configuration of a flow may consist of egress queue, the DSCP or CoS/802.1p value, and actions on out of profile (excess) traffic.

- Disable Mode—In this mode all traffic is mapped to a single best effort queue, so that no type of traffic is prioritized over another.

Only a single mode can be active at a time. When the system is configured to work in QoS Advanced mode, settings for QoS Basic mode are not active and vice versa.

When the mode is changed, the following occurs:

- When changing from QoS Advanced mode to any other mode, policy profile definitions and class maps are deleted. ACLs bonded directly to interfaces remain bonded.
- When changing from QoS Basic mode to Advanced mode, the QoS Trust mode configuration in Basic mode is not retained.
- When disabling QoS, the shaper and queue setting (WRR/SP bandwidth setting) are reset to default values.

All other user configurations remain intact.

SNMP

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a MIB. The SNMP manager can be part of a network management system (NMS) such as CiscoWorks. The agent and MIB reside on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

SNMP usually is associated with managing routers, but it’s important to understand that it can be used to manage many types of devices. The switch functions as SNMP agent and supports SNMPv1, v2, and v3.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository

for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

SNMP Versions

The Internet Engineering Task Force (IETF) is responsible for defining the standard protocols that govern Internet traffic, including SNMP. The IETF publishes Requests for Comments (RFCs), which are specifications for many protocols that exist in the IP realm. Documents enter the standards track first as proposed standards, then move to draft status. When a final draft is eventually approved, the RFC is given standard status—although there are fewer completely approved standards than you might think. Two other standards-track designations, historical and experimental , define (respectively) a document that has been replaced by a newer RFC and a document that is not yet ready to become a standard. The following list includes all the current SNMP versions and the IETF status of each.

- SNMP Version 1 (SNMPv1) is the initial version of the SNMP protocol. It's defined in RFC 1157 and is a historical IETF standard. SNMPv1's 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 a device's management information. There are typically three communities in SNMPv1: read-only, read-write, and trap. It should be noted that while SNMPv1 is historical, it is still the primary SNMP implementation that many vendors support.
- SNMP version 2 (SNMPv2) is often referred to as community-string-based SNMPv2.
- SNMP version 3 (SNMPv3) is the latest version of SNMP. Its main contribution to network management is security. It adds support for strong authentication and private communication between managed entities.

To control access to the system, a list of community entries is defined. Each community entry consists of a community string and its access privilege. The system responds only to SNMP messages specifying the community which has the correct permissions and correct operation.

SNMP agents maintain a list of variables that are used to manage the device. These variables are defined in the Management Information Base (MIB).

Table 8: SNMP Versions and Security Levels

Version	Level	Authentication	Encryption
SNMPv1	noAuthNoPriv	Community string	No
SNMPv2C	noAuthNoPriv	Community string	No
SNMPv3	noAuthNoPriv	Username	No
SNMPv3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No

Version	Level	Authentication	Encryption
SNMPv3	authPriv(requires the cryptographic software image)	MD5 or SHA	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)

Note Due to the security vulnerabilities of other versions, it is recommended to use SNMPv3.

SNMP Agent Functions

The SNMP agent responds to SNMP manager requests as follows:

- Get a MIB variable—The SNMP agent begins this function in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Set a MIB variable—The SNMP agent begins this function in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

The SNMP agent also sends unsolicited trap messages to notify an NMS that a significant event has occurred on the agent. Examples of trap conditions include, but are not limited to, when a port or module goes up or down, when spanning-tree topology changes occur, and when authentication failures occur.

SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the NMS to access the switch, the community string definitions on the NMS must match at least one of the three community string definitions on the switch.

A community string can have one of these attributes:

- Read-only (RO)—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access
- Read-write (RW)—Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings.
- When a cluster is created, the command switch manages the exchange of messages among member switches and the SNMP application. The Network Assistant software appends the member switch number (*@esN*, where *N* is the switch number) to the first configured RW and RO community strings on the command switch and propagates them to the member switches.

Supported MIBs

Management Information Base (MIBs) are collections of definitions which define the properties of the managed object within the device to be managed. For a list of supported MIBs, visit the following URL and navigate to the download area listed as Cisco MIBS:

http://www.cisco.com/cisco/software/navigator.html

Configure Switchport Mode Via SNMP

To configure switchport mode via SNMP on your switch, follow these steps:

Procedure

Step 1 Connect the switch via console port and reset the switch back to factory default.

Step 2 Enable SNMP and configure the community name for Read and Write privilege.

Step 3 From a MIB browser of choice (I.e: MG-Soft), select vlanPortModeState and right click.

Step 4 Next, select **Set**.

Step 5 The Select Table Instance(s) will appear. The table will include an instance ID which corresponds to an interface ID and the Value column value which corresponds to the switch port.

Example:

Instance 1 is for interface GigabitEthernet 1/0/1

Example:

Instance 3 is for Interface GigabitEthernet 1/0/3.

The Value indicates that the interface switchport mode is accessed.

General mode	10	Private-VLAN permiscouos mode	13
Access mode	11	Private-VLAN host mode	14
Trunk mode	12	Customer	15

Step 6 Select **Instance 3** and change the interface GigabitEthernet 1/0/3 switchport mode to General.

Step 7 Then, repeat the steps for trunk mode.

Create or Add a VLAN Via SNMP

To create or add a VLAN on your switch, follow these steps:

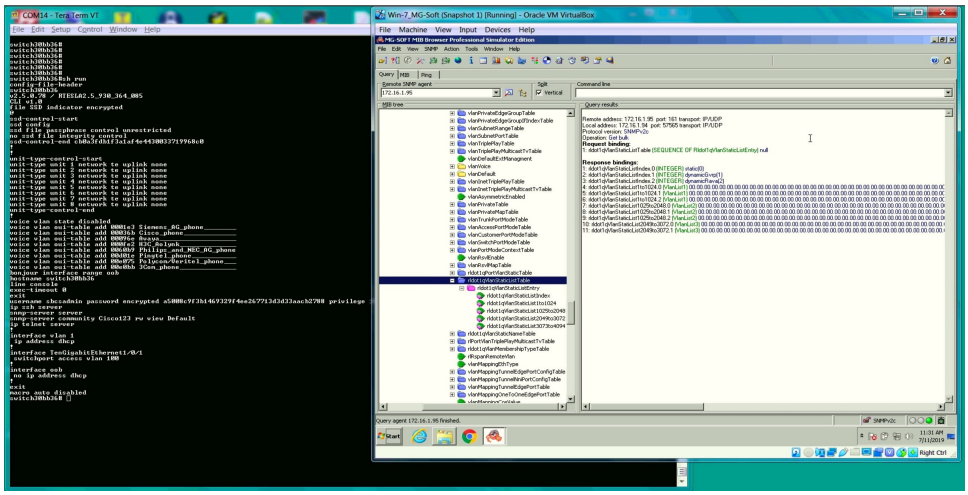
Procedure

Step 1 Connect the switch via a console port and reset the switch back to factory default.

Step 2 Enable SNMP and configure the community name for Read and Write privilege.

Step 3 Run a show run command.

Step 4 From MIB browser of choice, I am using MG-Soft, select rldot1qVlanStaticListTable MIB container and run Get Bulk operation.



Step 5 Refer to the slide above to create or add a VLAN.

a) Add VLANs 2-14, 16.

b) Select rldot1qVlanStaticList1to1024.

c) Open “Set” operation window.

d) Set the VLAN values in Octet format ”# 0x7F 0xFD.

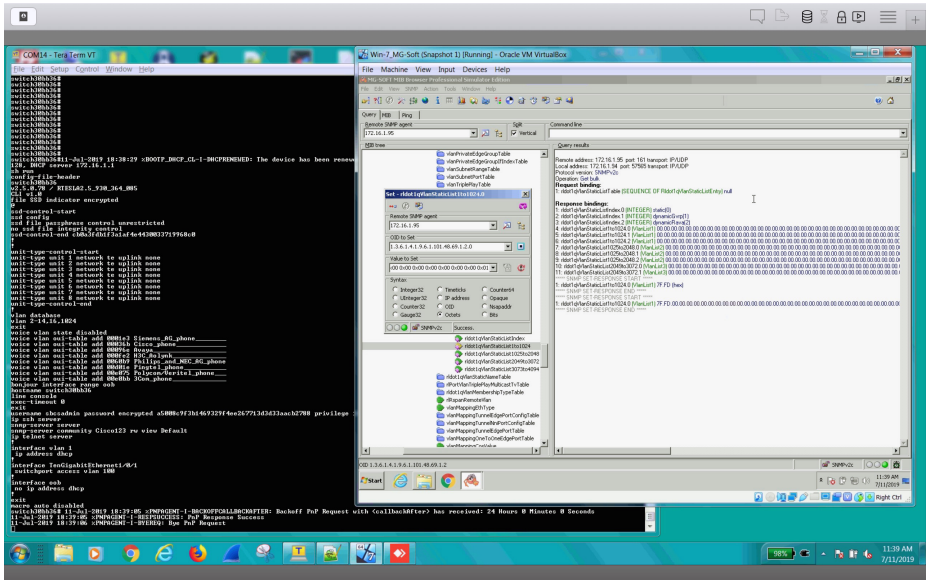
Example:

VLAN ID. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Octet bits 0 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1

Octet in Hex 7 F F D

Step 6 Click **Set** to add the VLANs.



Step 7 Complete the following if you wish to add an extra VLAN 1024.

a) With the Set operation window open, click on **Value to Set** to refresh icon. The field will be updated with "rldot1qVlanStaticList1to1024.
b) Right scroll inside the field until the last octet to set 1024th bit value to 1.
c) Click **Set**

There are 4 self explanatory VLAN lists:

- rldot1qVlanStaticList1to1024
- rldot1qVlanStaticList1025to2048
- rldot1qVlanStaticList2049to3072
- rldot1qVlanStaticList3073to4094

Reboot Reset Via SNMP

To reset the switch back to factory default settings, follow these steps:

Procedure

Step 1 Connect the switch via console port and reset the switch back to factory default.

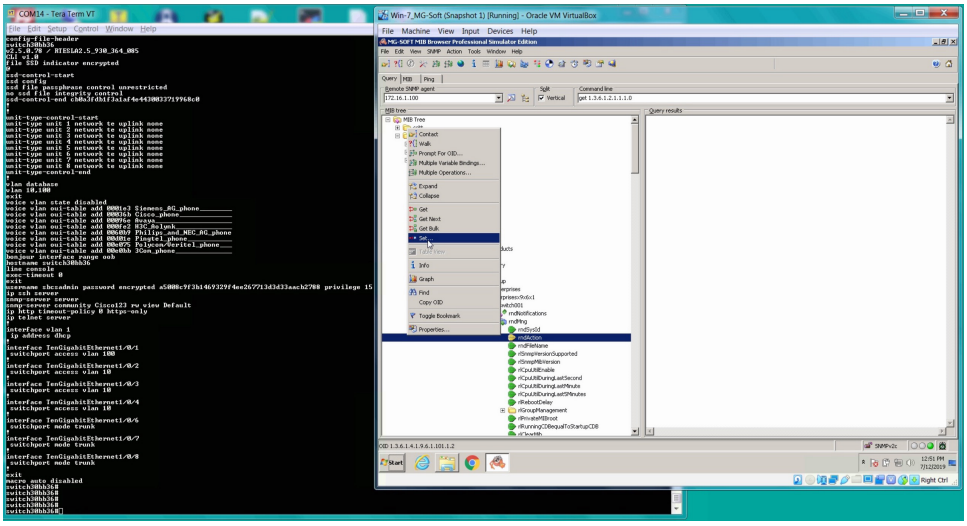
Step 2 Enable SNMP and configure community name for Read and Write privelege.

Step 3 Save the configuration.

Step 4 Run show command.

Step 5 From MIB browser of choice (i.e. MG-Soft), select rndAction MIB.

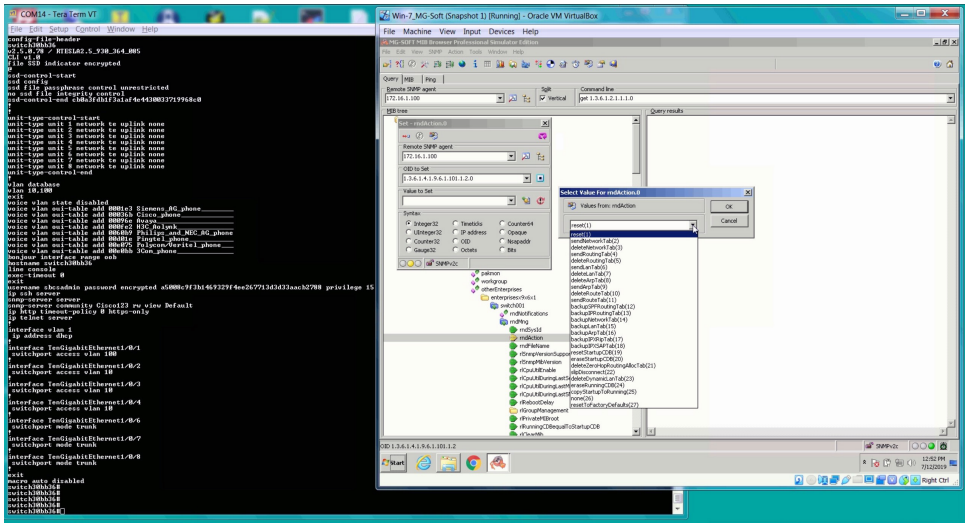
Step 6 Right click and select Set.



Step 7 Next to the Value to Set field, you will find 2 icons.

a) Click **Select From Value List**.
b) From the drop-down list, select **Reset** and click **OK**.

c) Next, click **Set**.



d) After the switch reboots, login with username and password and repeat the steps by selecting **resetTo Factory Default(27)**. After the reboot, you will need to create a new username and password.

