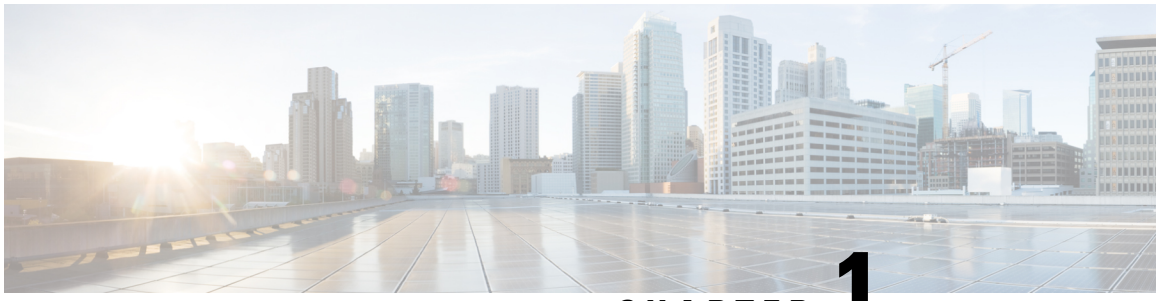
Cisco Business 220 Series Switches Administration Guide

First Published: 2020-12-08

Last Modified: 2021-07-20

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



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
- PoE Consideration, on page 5
- Front Panel, on page 6
- Configuring Switches, on page 8

Introduction

Thank you for purchasing the Cisco CBS 220 Series Switch. The Cisco CBS 220 Series Switches are the next generation of affordable smart switches that 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, and rich security capabilities. With an easy-to-use web user interface and Power over Ethernet Plus capability, you can deploy and configure a complete business network in minutes.

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 face of screw head to 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.

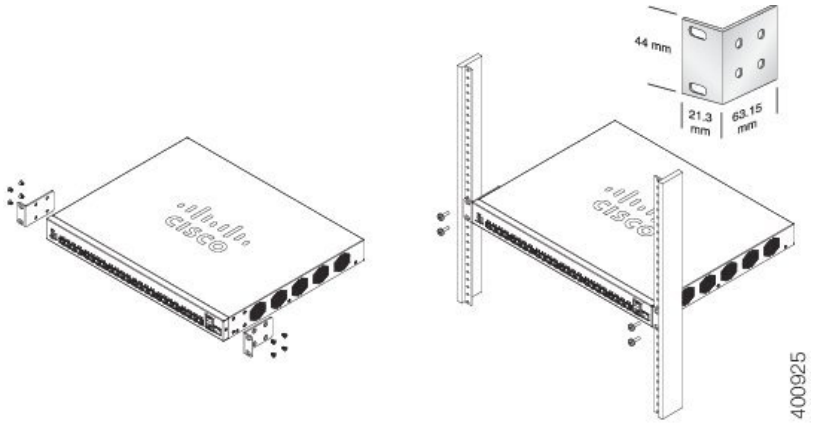
Caution For stability, load the rack from the bottom to the top, with the heaviest devices on the bottom. A top-heavy rack is likely to be unstable and might tip over.

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

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.



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, wallmount the switch with its front panel facing down or to the side to prevent airflow restriction and to provide easier access to the cables.

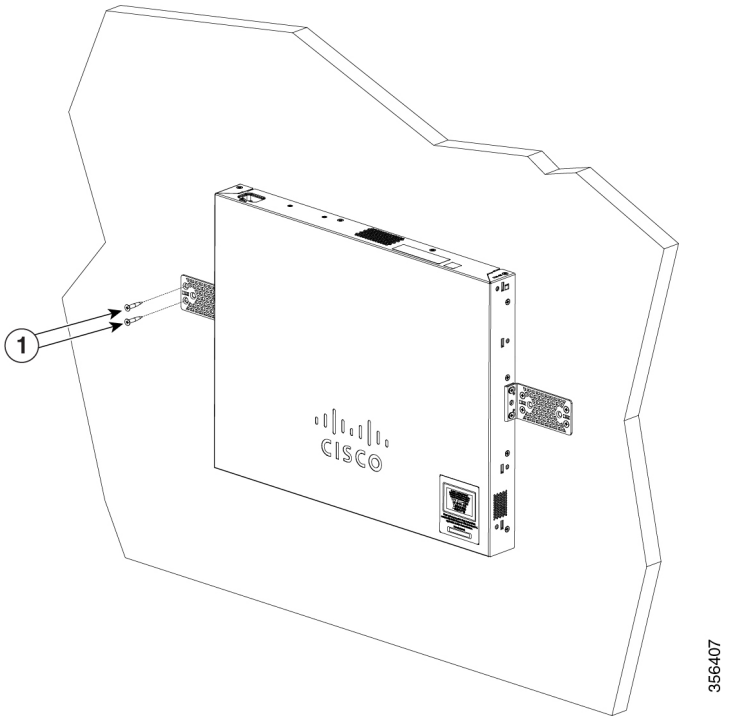
To wall-mount a 24-port switch using brackets:

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:

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 plywoodmounting backboard.

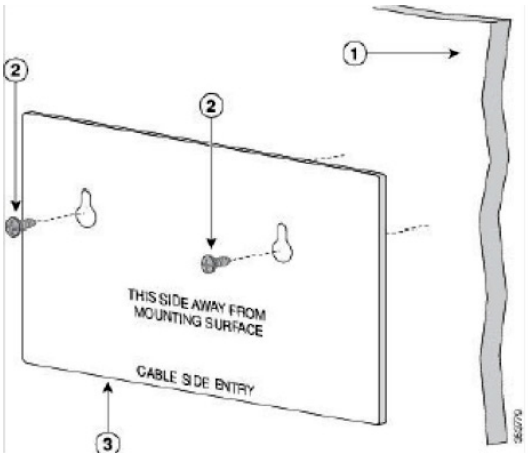
Step 3 Peel the adhesive strip off the bottom of the screw template.

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

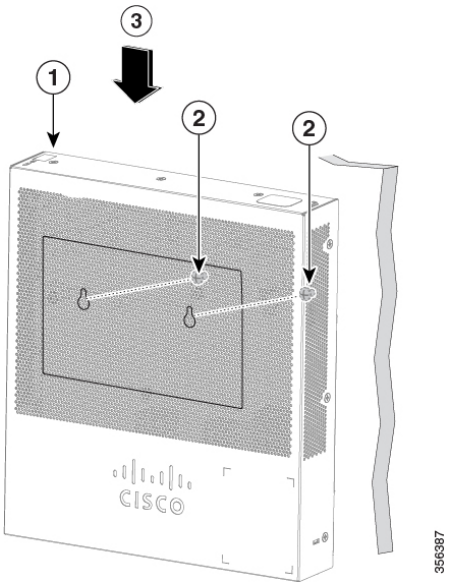
Figure 3 Installing the mounting screws on the wall



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



PoE Consideration

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.

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

Table 1: Switches with Power Over Ethernet

SKU Name	Description	PoE PD Chipset Type	PoE PSE Support
CBS220-8P-E-2G	10-Port Gigabit PoE Smart Switch	1*69208M	AF/AT
CBS220-8FP-E-2G	10-Port Gigabit PoE Smart Switch	1*69208M	AF/AT
CBS220-16P-2G	18-Port Gigabit PoE Smart Switch	2*69208M	AF/AT
CBS220-24P-4G	24-Port Gigabit PoE Smart Switch	3*69208M	AF/AT
CBS220-24FP-4G	24-Port Gigabit PoE Smart Switch	3*69208M	AF/AT
CBS220-48P-4G	48-Port Gigabit PoE Smart Switch	6*69208M	AF/AT
CBS220-48P-4X	48-Port Gigabit PoE Smart Switch	6*69208M	AF/AT
CBS220-48FP-4X	48-Port Gigabit PoE Smart Switch	6*69208M	AF/AT

Note 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 220 Series Model

Note Models may differ within the CBS 220 series and this is just a representation of a model within the series.

- Console port with RJ-45. The console connects a serial cable to a computer serial port so that it can be configured using a terminal emulation program.

  Note Only certain models support this feature.

- 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 10 GigaBit Interface Converter ports. The term SFP+ is used in this guide.
  - 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.
  - Small form-factor pluggable (SFP) ports are connection points for modules, so the switch can link to other switches.
- Reset button is used to reset or reboot the switch. To reboot the switch, press the Reset button for less than 10 seconds.

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 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.
- XG—(Green) (if present) 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) (if present) 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.
- 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.

Configuring Switches

The switch can be accessed and managed by two different methods; 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.

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:

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**.

If this is the first time that you have logged on with the default username and password, the Change username and Password page opens. The rules for constructing a new password are displayed on the page.

Step 8 Enter a new username and password and confirm.

Note Password complexity is enabled by default. The password must comply with the default complexity rules.

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, proceed with the following steps:

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 HyperTerminal 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.

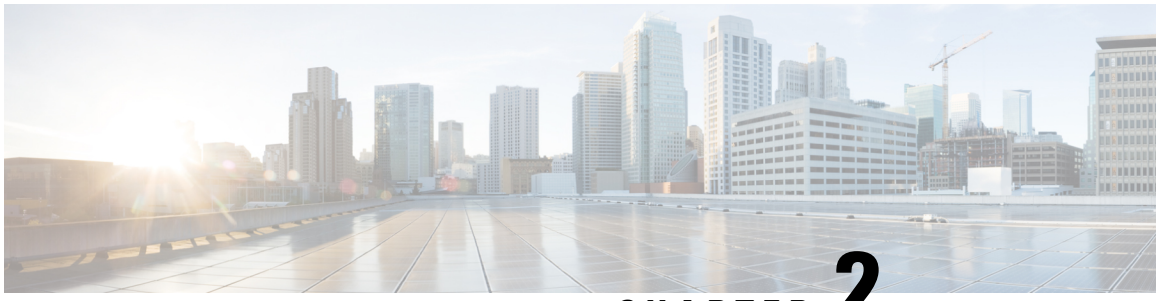
Caution Make sure that any configuration changes made are saved before exiting.

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 console.



CHAPTER 2

Getting Started

This chapter contains the following section:

- Getting Started, on page 11

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.

Initial Setup

Change Management Applications and Services	TCP/UDP Services, on page 129
Change Device IP Address	IPv4 Interface, on page 116
Create VLAN	VLAN Settings, on page 82
Configure Port Settings	Port Settings, on page 47

Device Status

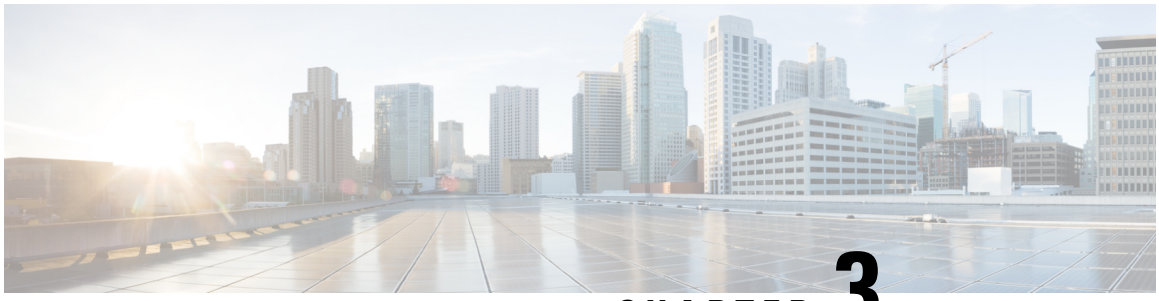
System Summary	System Summary, on page 13
Port Statistics	Interface, on page 13
RMON Statistics	RMON Statistics, on page 18
View Log	RAM Memory, on page 22

Quick Access

Change Device Password	User Accounts, on page 26
Upgrade Device Software	Firmware Operations, on page 34

Backup Device Configuration	File Operations, on page 35
Create MAC-Based ACL	MAC-Based ACL, on page 153
Create IP-Based ACL	IPv4-based ACL, on page 155
Configure QoS	QoS Properties, on page 163
Configure SPAN	SPAN and RSPAN, on page 16

There are two 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.



CHAPTER 3

Status and Statistics

This chapter contains the following sections:

- System Summary, on page 13
- Interface, on page 13
- Etherlike, on page 14
- Hardware Resource Utilization, on page 15
- Health, on page 16
- SPAN and RSPAN, on page 16
- RMON, on page 18
- View Log, on page 22

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**.

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:

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.
  - Select the refresh rate from the Refresh Rate drop-down menu.

- Select an interface and click **Clear Interface Counters** to clear the statistics counters for the selected interface.
- Click **Clear All Interface Counters** to clear the statistics counters for all interfaces.
- Select an interface and click **View Interface Statistics** to see the statistics counters for the selected interface on a single page.
- Click **Refresh** to manually refresh the statistics counters for all interfaces.

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:

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

Step 2 To view statistics counters in table view, click **View All Interfaces Statistics** to see all ports in table view.

- Select the refresh rate from the Refresh Rate drop-down menu.
- Select an interface and click **Clear Interface Counters** to clear the statistics counters for the selected interface.

- Click **Clear All Interface Counters** to clear the statistics counters for all interfaces.
- Select an interface and click **View Interface Statistics** to see the statistics counters for the selected interface on a single page.
- Click **Refresh** to manually refresh the statistics counters for all interfaces.

Step 3 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 - Received flow control pause frames.
- Pause Frames Transmitted - Number of flow control pause frames transmitted from the selected interface.

Step 4 You can also click **Refresh** to refresh the stats or click **Clear Interface Counters** to clear 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.

The count of each item may differ from different Models due to system design. Also, because of ASIC characteristics, it’s possible to show a "Lack of HW resources" when binding an Advance QoS service policy or User-defined ACL but this page shows enough TCAM resources.

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

The following fields are displayed:

- Total Entries
  - Maximum—Number of available TCAM entries that can be used for whole system.
  - In Use—Number of TCAM entries used for whole system
- System Rules
  - Allocated—Number of allocated TCAM entries that can be used for system rules.

- In Use—Number of TCAM entries used for system rules.

- ACL and QoS Rules
  - Allocated—Number of allocated TCAM entries that can be used for ACL and QoS rules.
  - In Use—Number of TCAM entries used for ACL and QoS rules.

Health

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

Fan Status

- Fan—Displays fan ID.
- Status—Displays whether the fan is operating normally (OK) or not (Fault).
- Speed (RPM)—Displays fan speed.

Temperature Status

- Sensor—Displays sensor id.
- Status—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.
- TEMP (°C) —Displays temperature of sensor.

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, multipledevice 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.

RSPAN supports source ports, source VLANs, and destination ports on different switches, enabling remote monitoring of multiple switches across your network. 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

RSPAN traffic from the source ports or VLANs is copied into the RSPAN VLAN and forwarded carrying the RSPAN VLAN to a destination session monitoring the RSPAN VLAN.

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.

RSPAN VLAN

An RSPAN VLAN carries SPAN traffic between RSPAN source and destination sessions.

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

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

Step 2 Select the RSPAN VLAN.

Step 3 Click **Apply**.

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:

Step 1 Click **Status and Statistics** >**SPAN & RSPAN**> **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.
- Destination Type – Select a local interface or remote VLAN as destination.
- Port—Select a port from the drop-down list.
- Network Traffic—Select to enable that traffic other than monitored traffic is possible on the port.

Step 4 Click **Apply**.

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 any number of source ports (up to the maximum number of available ports on the switch) and any number of source VLANs.

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

Step 1 Click **Status and Statistics** > **SPAN and RSPAN** > **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 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 5 Click **Apply**. The source interface for the mirroring is configured.

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).

RMON 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:

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.

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

Step 4 To view counters in table view:

- Click **View All Interfaces Statistics** to see all ports in table view.

RMON 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:

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.

RMON Events

The Events page displays the log of events (actions) that occurred. Two types of events can be logged: Log or Log and Trap. The action in the event is performed when the event is bound to an alarm and the conditions of the alarm have occurred.

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

Step 2 Click **Add**.

Step 3 Enter the parameters:

- Event Entry—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—Entera 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 goesoff.
  - Log (Event Log Table)—Add a log entry to the Event Log table when the alarm istriggered.
  - 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:

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.

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.
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.

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.

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.

- 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 Index—Log entry number
- 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 32. Flash logs remain when the device is rebooted. You can clear the logs manually.

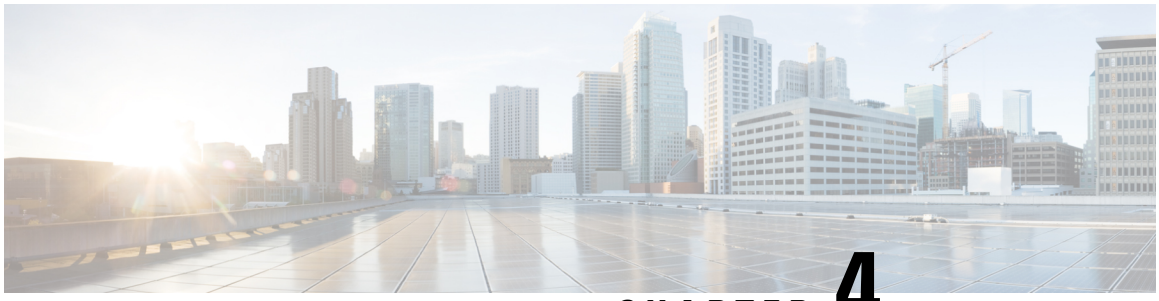
To view the Flash logs, click **Status and Statistics** > **View Log** > **Flash Memory**.

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 4

Administration

This chapter contains the following sections:

- System Settings, on page 25
- Console Settings , on page 26
- User Accounts, on page 26
- Idle Session Timeout, on page 27
- Time Settings, on page 28
- System Log, on page 31
- File Management, on page 33
- Cisco Business Dashboard Settings, on page 37
- Plug-n-Play (PNP), on page 38
- Reboot, on page 43
- Diagnostics, on page 43
- Discovery Bonjour, on page 46
- Discovery LLDP, on page 46
- Discovery - CDP, on page 58
- Locate Device, on page 64
- Ping, on page 64
- Traceroute, on page 65

System Settings

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

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 2000 characters.

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

Console Settings

The console port speed can be set to one of the following speeds: 2400, 4800, 9600, 19200, 38400, 57600, and 115200.

To configure the console settings, follow these steps:

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

Step 2 Select a value from the Console Port Baud Rate drop-down menu. The available values are 2400, 4800, 9600, 19200, 38400, 57600, and 115200 Bit/sec.

Step 3 Click **Apply**. The console port Baud rate is defined, and the Running Configuration is updated.

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:

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

Step 2 Click **Add** to add a new user or click **Edit** to modify a user.

Step 3 Enter the parameters.

- User Name—Enter a new username from 0 through 31 characters. UTF-8 characters aren't permitted.
- Password—Enter a password (UTF-8 characters aren't permitted).
- Confirm Password—Enter the password again.
- Password Strength Meter—Displays the strength of password. The password must comply with the minimum strength and complexity requirements shown on this page.
- 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/Write Management Access (15)—User can access the GUI, and can configure the device.

Step 4 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-256 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:

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

Step 2 Select the timeout for the 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

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.

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:

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

The following fields are displayed:

- Actual Time— Actual system time on the device.

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.
- 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
  - 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 Settings

The switch can be configured to synchronize its system clock with an SNTP server specified on the SNTP Settings page.

To specify an SNTP server by name, you must first configure the DNS servers on the switch and enable the Main Clock Source (SNTP Servers) on the System Time page.

To add a SNTP server, complete the following steps:

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

Step 2 Enter the following information:

- Host Definition—Select whether to specify the SNTP server by IPv4 address or by host name.
- SNTP Server IP Address/Name—Enter the IPv4 address or hostname of the SNTP server.

Step 3 Click **Apply**. The SNTP server is added, and the Running Configuration is updated

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

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.

Periodic Time Range

A periodic 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 periodic time range element to an absolute time range:

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

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

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

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

Step 4 Enter the following fields:

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

Step 5 Click **Apply.**

Step 6 Click **Time Range** to access the Time Range, on page 30.

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

You can select the events to be logged by severity level. Each log message has a severity level concatenated with a dash (-) on each side. For example, the log message "SYSTEM-5-STARTUP: … " has a severity level of 5, meaning Notice.

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.

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:

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

Step 2 Enter the parameters.

Logging	Select to enable message logging.
Syslog Aggregator	Select 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.
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 Log Servers

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:

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

Step 2 Click **Add**.

Step 3 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.
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.
Minimum Severity	Select the minimum level of system log messages to be sent to the server.

Step 4 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. Various actions can be performed with these files, such as: selecting the firmware file from which the device boots, 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.

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

The following fields are displayed:

- Active Image—Displays the current, active firmware file.
- Active Image Version Number—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 Transfer 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.
TFTP	For TFTP, proceed with the TFTP Instructions below.

TFTP Instructions

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

TFTP Server IP Address/Name	Select from the following options: • By IP Address • By Name
IP Version	Select from the following options: • IP Version 6 • IP Version 4
TFTP Server IP Address/Name	Enter the server IP address/name.
Source File Name	Enter the name of the source (0 - 128 characters used)

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

File Operations

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
- Backup Configuration
- Mirror Configuration
- Logging File
- Language 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.
TFTP	For TFTP, proceed with the TFTP Instructions below.

TFTP Instructions

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

TFTP 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
TFTP Server IP Address/Name	Enter the server IP address/name.
Source File Name	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**.

Configuration File Properties

The Configuration File Properties page displays the system files existing in the system.

Step 1 Click **Administration** > **File Management** > **Configuration File Properties**.

Step 2 If required, select either the Startup Configuration, Backup Configuration, or both and click delete icon to delete these files.

DHCP Auto Configuration

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

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

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.

Step 3 Select the TFTP server settings.

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
Backup TFTP Server IP Address/Name	Enter the name of the backup configuration file.
Backup Configuration File	Enter the name of the backup configuration file (0 - 160 characters used)
Last Auto Configuration TFTP Server IP Address	The address of the last auto configuration 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.

Note For detailed instructions on how to setup the Cisco Business Dashboard Manager and Agent, 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 an Agent connection to a Dashboard, configure the Organization and Network name, and other information required to allow connection to the Dashboard:

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

Step 2 Configure the following:

Connection Status	Displays the status of the Cisco Business Dashboard connection.
Agent Version	Displays the version of the Cisco Business Dashboard call home agent.

Callhome Agent Enabled	Check to enable call home agent for connecting to Cisco Business Dashboard.
Callhome Agent Log Level	Select the logging severity of call home agent.
Dashboard Connection Enabled	Check to enable connectivity.
Organization Name	Enter the organization name of the Cisco Business Dashboard Agent running on the device.
Network Name	Enter the site name of the Cisco Business Dashboard Agent.
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 hostname to the IP Address/Name field.
IP Address/Name	Enter the name of 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.
Access Key ID	Specify the key ID to be used for the initial authentication between the Cisco Business Dashboard Agent running on the device and the Cisco Business Dashboard.
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.

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.

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 hostname "pnpserver" - the PnP server IP addressed is obtained via DNS server resolution of hostname “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 trustpool 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 uninstalled.

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 hostname/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.

Parameter	Description
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 hostname of PnP server. If hostname is specified, DNS related options must be present in the DHCP server to allow for successful use of hostname.
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;J443;Thttp://10.10.10.3/ca/trustpool/ios.p7b;Z10.75.166.1
```

PNP Settings

To configure PNP settings, follow these steps:

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: • Auto—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. • Static—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 IP Address/Name	Enter the IP address or domain name of the PNP server.

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

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:

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 Address—IP address of PNP server

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:

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.
- 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.

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

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

Step 1 Click **Administration** > **Diagnostics** > **Copper Test**.

Step 2 Select a 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:

- Test Results—Cable test results. Possible values are:
- Cable Length—Estimated cable length. The cable length is Unknown when the green features are enabled.
- Operational Port Status—Displays whether port is up or down.

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-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

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

This page displays the following fields:

- Port—Port number on which the SFP is connected
- 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
- Loss of Signal—Local SFP reports signal loss. Values are True and False

CPU Utilization

To view the current CPU utilization and/or set the refresh rate:

Step 1 Click **Administration >Diagnostic > 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.

Tech-Support Information

This page provides a detailed log of the device status. This is valuable when the technical support are 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:

Step 1 Click **Administration**> **Diagnostics** > **Tech-Support Information**.

Step 2 Click **Generate**.

Note Generation of output from this command may take some time. When the information is generated, the tech-support information file will be download to default download directory of browser automatically.

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:

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

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

Step 3 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.

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. To enter LLDP properties, proceed as follows:

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. • Bridging— (VLAN-aware flooding) Forwards the packet to all VLAN members. • 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.
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.

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

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 49.

To define the LLDP port settings, follow these steps:

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.
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 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 • Management IP Address

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 49. 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.

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

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

This page contains previously-created network policies.

Step 2 Check **Enable** next to the LLDP MED Network Policy for Voice Application option to automatically generate and advertise a network policy for voice application based on the voice VLAN maintained by the device.

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 Tag—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

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 enabled 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:

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 48. 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.
- 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.

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:

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

- Address Subtype—Type of management IP address that is listed in the Management Address field, for example, IPv4.
- Address—Returned address most appropriate for management use, typically a Layer 3 address.
- Interface Subtype—Numbering method used for defining the interface number.
- Interface Number—Specific interface associated with this management address.

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.

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

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:

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

Step 2 Select a local port, and click **Go**.

The following fields are displayed:

- 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.

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.
- 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 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.

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.

VLAN ID Table

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

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.

Step 4 Click **Refresh** to refresh the data in the LLDP Neighbor table.

LLDP Statistics

The LLDP Statistics page displays LLDP statistical information per port.

To view the LLDP statistics, follow these steps:

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 age outs on the interface.

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

LLDP Overloading

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:

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 directly connected 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:

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—(VLAN-aware flooding) Forwards the packet based on the VLAN • Filtering—Deletes the packet • Flooding—(VLAN-unaware flooding) 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.
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 CDP 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, hostname).
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 CDP properties are defined.

CDP Interface Settings

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 protocol.

To define the CDP interface settings:

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

This page displays the following CDP information for each interface.

- Entry No.—Port identifier.
- 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 61 .
- CDP Neighbor Information Details—Takes you to the CDP Neighbors Information, on page 62.

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:

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	Address—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 (Only applicable for PoE models)	• 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.

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:

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.
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.

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.

Note Disconnects on the Clear Table button all connected devices if from CDP.

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:

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).

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.

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:

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.
Host IP Address/Name	Enter the IP address or hostname of the host to be pinged.

Option	Description
Number of Pings	The number of times the ping operation is performed. Select to use the default or specify your own value.

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, Ping aborted, Ping in progress by another process, 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.

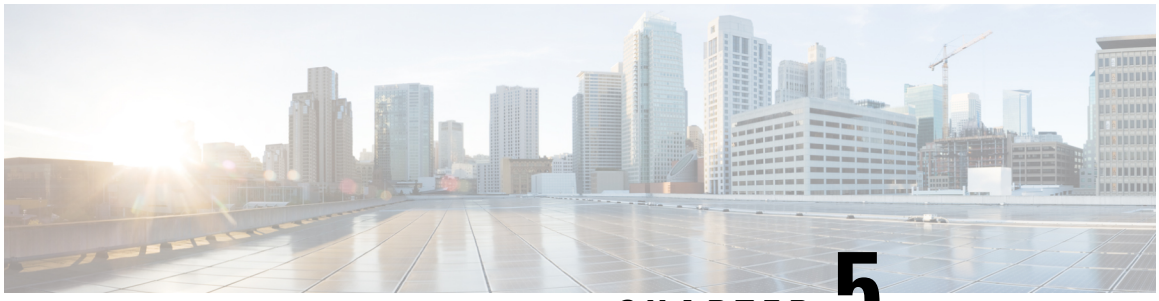
Step 1 Click **Administration** > **Traceroute**.

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

- Host Definition—Select whether hosts are identified by their IP address or name.
- 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**.

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.



CHAPTER 5

Port Management

This chapter contains the following sections:

- Port Settings, on page 67
- Error Recovery Settings, on page 70
- Loopback Detection Settings, on page 71
- Link Aggregation, on page 71
- Power over Ethernet, on page 75
- Green Ethernet, on page 78

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:

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

The port settings are displayed for all ports.

Step 2 Enter the following fields:

- Jumbo Frames—Check to support packets of up to 10 KB in size. If Jumbo Frames isn't enabled (default), the system supports packet size up to 1522 bytes.

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 35, 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.

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.
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
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.
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 or 10G, 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 Speed	Select the capabilities advertised by auto-negotiation when it is enabled. **Note** Not all options are relevant for all devices. The options are: • All Speed—All port speeds and duplex mode settings can be accepted. • 10M—10 Mbps speed • 100M—100 Mbps speed • 1000M—1000 Mbps speed • 10M/100M—10 and 100 Mbps speeds • 10G—10 Gbps speed
Operational Advertisement	Displays the capabilities currently published to the ports neighbor. The possible options are those specified in the Administrative Advertisement field.
Auto Advertisement Duplex	Select the duplex mode to be advertised by the port. The options are: • All Duplex—All duplex modes can be accepted. • Full—The interface supports transmission between the switch and the client in both directions simultaneously. • Half—The interface supports transmission between the switch and the client in only one direction at a time
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.
Protected Port	Check Enable 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 Link Aggregation Groups (LAGs)) that share the same Broadcast domain (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.Both ports and LAGs can be defined as protected or unprotected.

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:

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
  - 802.1x Single Host Violation—Select to enable automatic error recovery when the port is shut down by 802.1x.
  - ACL —Select to enable automatic error recovery mechanism by an ACL action.
  - BPDU—Enable automatic recovery when the port is shut down by STP Loopback Guard.
  - Broadcast Flood—Select to enable automatic error recovery from the Broadcast flood
  - DHCP Rate Limit—Check Enable to enable the timer to recover from the DHCP rate limit causes.
  - ARP Inspection—Check Enable to the timer to recover from the ARP inspection causes
  - PoE— Select Enable to enable the timer to recover from the Power over Ethernet (PoE) causes
  - Loopback Detection—Select to enable error recovery mechanism for ports shut down by loopback detection.
  - Port Security—Select to enable automatic error recovery when the port is shut down for port security violations.
  - Self Loop—Select Enable to enable the timer to recover from the self loop cause
  - Unicast Flood— Select Enable to enable the timer to recover from the Unicast flood causes.
  - Unknown Multicast Flood— Select Enable to enable the timer to recover from the unknown Multicast flood causes.

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:

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.

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:

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.
- 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:

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.
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 go to Time Range, on page 30
Operational Status	Displays whether the LAG is currently operating.
Operational Time Range State	Displays whether the time range is currently active or inactive.
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 Port Speed	Select the speed of the ports in the LAG.
Back Pressure	Check the **Enable** check box in the Back Pressure area to slow down packet reception speed when the device is congested. This feature is used with half duplex mode, and disables the remote port by preventing it from sending packets and jamming the signal.
Auto Advertisement Speed	Select the capabilities to be advertised by the LAG. The options are: • All Speed—All LAG speeds and both duplex modes are available. • 10M—The LAG advertises a 10 Mbps speed and the mode is full duplex. • 100M—The LAG advertises a 100 Mbps speed and the mode is full duplex. • 1000M—The LAG advertises a 1000 Mbps speed and the mode is full duplex. • 10/100M—The LAG advertises a 10/100 Mbps speed and the mode is full duplex. • 10G—The LAG advertises a 10G speed and the mode is full duplex.

Option	Description
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.
Current Flow Control	Displays the current Flow Control setting.

Step 4 Click **Apply**. The Running Configuration file is updated.

Link Aggregation Control Protocol (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:

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.

Power over Ethernet

This section describes how to use the PoE feature.

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:

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 counters are displayed for the device:
  - Operational Status—Displays the operational status (Normal or Fault) of the PoE switch.
  - Nominal Power—Total amount of power the device can supply to all the connected PDs.
  - Consumed Power—Amount of power currently being consumed by the PoE ports.
  - Available Power—Nominal power minus the amount of consumed power.
- 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 Port 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:

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

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

Step 3 Enter the value for the following field:

- Interface—Select the port to configure.
- PoE 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. Time ranges are defined in Time Range, on page 30. Click **Edit** to go to the Time Range page.
- Power 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—If the Power mode is Port Limit, enter the power in milliwatts allocated to the port (Range: 0 - 30000. Default: 30000).
- 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.
- Power Consumption—Displays the amount of power in milliwatts assigned to the powered device connected to the selected port.
- 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
1	4.0 watt
2	7.0 watt
3	15.4 watt
4	30.0 watt

- Overload Counter—Displays the number of overload counters
- Short Counter—Displays the number of short counters
- Denied Counter—Displays the number of denied counters
- Absent Counter—Displays the number of absent counters
- Invalid Signature Counter—Displays the times that an invalid signature was received. Signatures are the means by which the powered device identifies itself to the PSE. Signatures are generated during powered device detection, classification, or maintenance.

Step 4 Click **Apply**. The PoE settings for the port are written to the Running Configuration file.

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 enable 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.

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.

Green Ethernet 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:

Step 1 Click **Port Management** > **Green Ethernet** > **Properties**.

Step 2 Enter the values for the following fields:

- 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.

Step 3 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 Green Ethernet Properties, on page 78.

To define per port Green Ethernet settings, follow these steps:

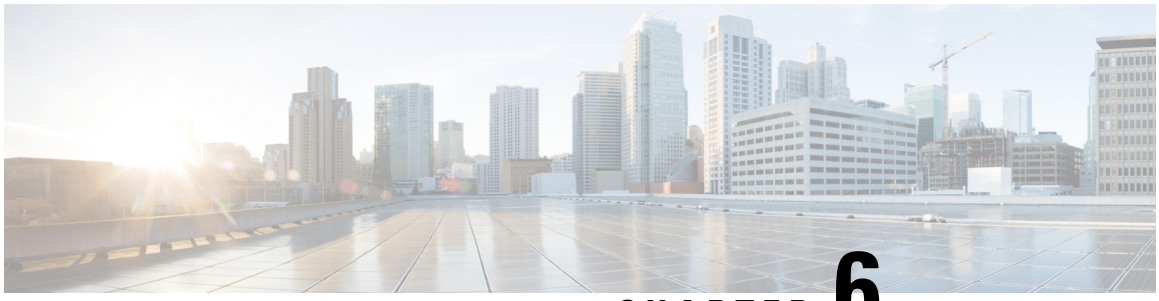
Step 1 Click **Port Management** > **Green Ethernet** > **Port Settings**.

The Port Settings page displays the following:

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

Step 3 Select to enable or disable 802.3 Energy Efficient Ethernet (EEE) mode on the port.

Step 4 Click **Apply**. The Green Ethernet port settings are written to the Running Configuration file.



CHAPTER 6

VLAN Management

This chapter contains the following sections:

- Default VLAN Settings, on page 81
- VLAN Settings, on page 82
- VLAN Interface Settings, on page 82
- Port to VLAN, on page 83
- Port VLAN Membership, on page 84
- GVRP Settings, on page 85
- Voice VLAN, on page 86

Default VLAN Settings

When using the factory default settings, the switch automatically creates VLAN 1 as the default VLAN, the default interface status of all ports is Trunk, and all port are configured as untagged members of the default VLAN.

The default VLAN has the following characteristics:

- Distinct, non-static, and non-dynamic, and all ports are untagged members by default.
- Cannot be deleted.
- Cannot be given a label.
- Cannot be used for any special role such as unauthenticated VLAN or voice VLAN. This is only relevant for OUI-enabled voice VLAN.
- If a port is no longer a member of any VLAN, the switch automatically configures the port as an untagged member of the default VLAN. A port is no longer a member of a VLAN if the VLAN is deleted or the port is removed from the VLAN.

When the VID of the default VLAN is changed, the switch performs the following on all ports in the VLAN

- Removes VLAN membership of the ports from the original default VLAN.
- Changes the PVID of the ports to the VID of the new default VLAN.
- Adds the ports as untagged VLAN members of the new default VLAN.

To change the default VLAN, complete the following steps:

Step 1 Click **VLAN Management > Default VLAN Settings**.

Step 2 Enter the following information:

- Current Default VLAN ID—Displays the current default VLAN ID.
- Default VLAN ID—Enter a new VLAN ID to replace the default VLAN ID.

Step 3 Click Apply. The default VLAN is changed, and the Running Configuration is updated.

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:

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 To add a range of VLANs, check **Range** and enter a VLAN Range (Range 2 - 4094) in the VLAN range field.

Step 5 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:

Step 1 Click **VLAN Management** > **Interface Settings.**

Step 2 Select an interface type (Port or LAG), and click **Go**. Ports or LAGs and their VLAN parameters are displayed.

Step 3 To configure a Port or LAG, select it and click **Edit.**

Step 4 Enter the values for the following fields:

Interface	Select a Port/LAG.
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. • Dot1q-Tunnel—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 dot1-q-tunnel ports.
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.
Administrative PVID	PVID for selected VLAN mode.
Uplink	(Available only in Trunk mode). Check **Enable** to set the interface as an uplink port.
TPID	(Available only in Trunk mode) If Uplink is enabled, select the TPID value for the interface.

Step 5 Click **Apply**.

Port to VLAN

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:

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.

Step 3 To change the registration of an interface to the VLAN, select the desired option from the following list:

- 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.
- PVID—Check to set the PVID of the interface to the VID of the VLAN. PVID is a per-port setting.

Step 4 Click **Apply**. The interfaces are assigned to the VLAN, and written to the Running Configuration file.

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.

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:

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 82.
- Administrative VLANs— Displays all VLANs of which the interface might be a member.
- Operational VLANs—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 82.
- Access Mode Membership (Active)
  - Access VLAN ID—Select the 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.
- Dot1q Tunnel Mode Membership
  - Dot1q Tunnel VLAN ID—When the port is in Dot1q Tunnel mode, it's a member of this 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.

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:

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.

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.

Voice VLAN 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).

To view and configure Voice VLAN properties:

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

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.

Telephony OUI

Organizationally Unique Identifiers (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:

Step 1 Click **VLAN Management** > **Voice VLAN** > **Telephony OUI**.

The Telephony OUI page contains the following fields:

- Telephony OUI—First six digits of the MAC address that are reserved for OUIs
- Description—User-assigned OUI description.

Step 2 Specify the following general Telephony OUI parameters

- 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 3 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 4 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.

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:

Step 1 Click **VLAN Management** > **Voice VLAN** > **Telephony OUI Interface**.

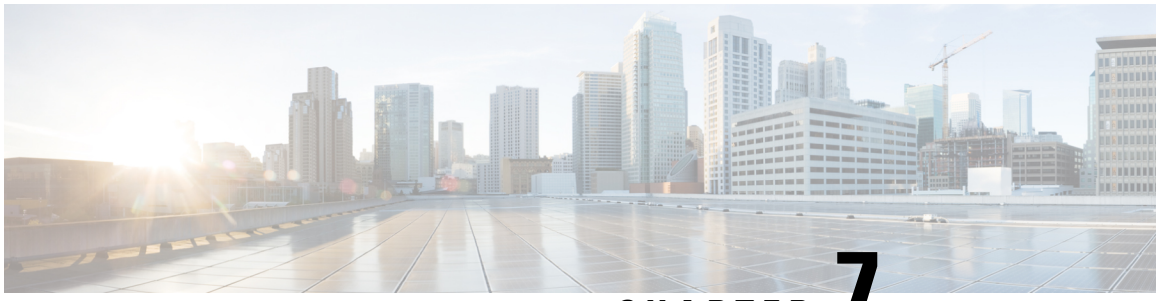
The Telephony OUI Interface page contains voice VLAN OUI parameters for all interfaces.

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.



CHAPTER 7

Spanning Tree

This chapter contains the following sections:

- STP Status and Global Settings, on page 91
- STP Interface Settings, on page 92
- RSTP Interface Settings, on page 94
- MSTP Properties, on page 95
- VLANs to MSTP Instance, on page 96
- MSTP Instance Settings, on page 97
- MSTP Interface Settings, on page 97

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:

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.
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:

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.
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 • Disable—Disables Fast Link
BDU Guard	If enabled, the interface will shut down when a BPDU message is received.
BDU Filter	If enabled, the interface will not send and receive BPDU messages.
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 bea 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. • 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.

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:

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.
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.
Port Status	Displays the RSTP status on the specific port. • Disabled-STP is currently disabled on the port. • Learning-The port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses. • Blocking-The port is currently blocked, and can't forward traffic (except for BPDU data) or learn 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 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 97. Use this page if the system operates in MSTP mode.

To define MSTP, follow these steps:

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.

Step 3 Click **Apply**. The MSTP properties are defined, and 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:

Step 1 Click **Spanning Tree** > **RSTP Interface Settings** > **MSTP** > **VLAN 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.

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:

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:

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.

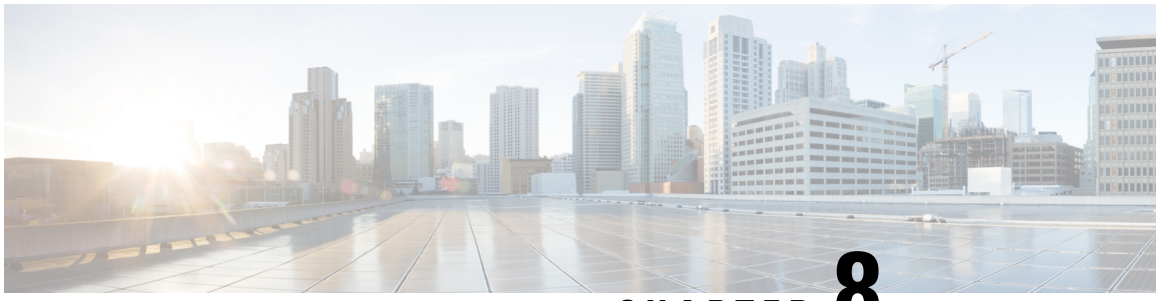
Step 4 Select an interface, and click **Edit**.

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. • Learning—The port on this instance is in Learning mode. The port cannot forward traffic, but it can learn new MAC addresses. • Blocking—The port is currently blocked, and can't forward traffic (except for BPDU data) or learn MAC addresses. • Forwarding—The port on this instance is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
Port Role	Displays the port or LAG role, per port or LAG per instance, assigned by the MSTP algorithm to provide STP paths: • Master—A Master port provides connectivity from an MSTP region to the outlying CIST root • 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.
Mode	Displays the current interface Spanning Tree mode. • If the link partner is using MSTP or RSTP, the displayed port mode is RSTP. • If the link partner is using STP, the displayed port mode is STP.
Type	Displays the MST type of the port.

Option	Description
	• 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.

Step 6 Click **Apply**. The Running Configuration file is updated.



CHAPTER 8

Mac Address Tables

This chapter contains the following sections:

- Static Addresses, on page 101
- Static Address Filtering, on page 102
- Dynamic Address Settings, on page 102
- Dynamic Addresses, on page 102
- Reserve MAC Address, on page 103

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:

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.

Static Address Filtering

Use the Static Address Filtering page to configure the static MAC address filter profiles so that specific MAC addresses will not be assigned to the specified VLANs on the switch. To define a static MAC address filter profile, complete the following steps:

Step 1 Click **MAC Address Tables > Static Address Filtering**.

Step 2 Click **Add**.

Step 3 Enter the following information:

- MAC Address—Enter the MAC address.
- VLAN ID—Select a VLAN ID. The specified MAC address will not be assigned to this VLAN.

Step 4 Click **Apply**. The static MAC address filter profile is added, and the Running Configuration is updated.

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:

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:

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**.

Reserve MAC Address

When the switch receives a frame using a destination MAC address that belongs to a reserved range (per the IEEE standard), the frame can be discarded or bridged.

Use the Reserved MAC Address page to define the MAC addresses to be reserved and the actions how to deal with the frame.

To reserve a MAC address:

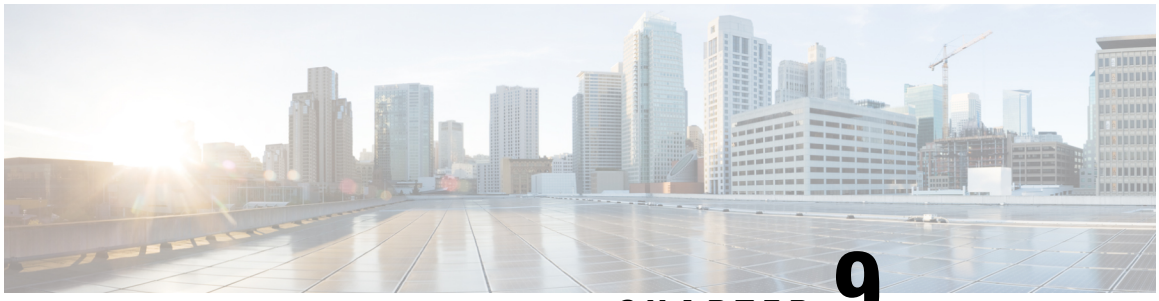
Step 1 Click **MAC Address Tables > Reserve MAC Addresses**.

Step 2 Click **Add**.

Step 3 Enter the following information:

- MAC Address—Select the MAC address to be reserved.
- Action —Select one of the following actions to be taken upon the arriving packet that matches the selected criteria:
  - Bridge—Forwards the packet to all VLAN members.
  - Discard—Deletes the packet

Step 4 Click **Apply**. The MAC address is reserved, and the Running Configuration is updated.



CHAPTER 9

Multicast

This chapter contains the following sections:

- Multicast Properties, on page 105
- IP Multicast Group Address, on page 106
- IGMP Snooping, on page 107
- MLD Snooping, on page 109
- IGMP/MLD Snooping IP Multicast Group, on page 110
- Multicast Router Port, on page 110
- Forward All, on page 111
- Maximum Multicast Groups, on page 112
- Multicast Filtering, on page 112

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 to239.255.255.255.
- The IPv6 Multicast address isFF00:/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 configure Multicast properties, follow these steps:

Step 1 Click **Multicast** > **Properties**.

Step 2 Enter the parameters.

IGMP Snooping	Enable or disable IGMP Snooping globally on the switch (enabled by default). When enabling IGMP Snooping, the devices that monitor network flow will determine which hosts have requested to receive multicast traffic, and the switch only executes IGMP Snooping.
MLD Snooping	Enable or disable MLD Snooping globally on the switch (disabled by default).
Unknown Multicast Action	Choose how to deal with unknown Multicast frames. The possible options are: • Drop—Drops unknown Multicast frames. • Flood—Floods unknown Multicast frames. • Forward to Router Port—Forwards unknown Multicast frames to Mrouter port.

Step 3 Click **Apply**. 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:

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).

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 IP Address—Defines the source address to be included.

Step 6 For each port, select its association type. The options are:

- Static—Attaches the port to the Multicast group as a static member.
- None—Indicates that the port is not currently a member of this Multicast group on this VLAN.

Step 7 Click **Apply**. The Running Configuration file is updated.

IGMP Snooping

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.

To support selective IPv4 Multicast forwarding, bridge Multicast filtering must be enabled (in Multicast Properties, on page 105). 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:

Step 1 Click **Multicast** > **IGMP Snooping**.

Step 2 Enter the following information:

- IGMP Snooping Version—Select either IGMPv2 or IGMPv3.
- Report Suppression—Enable or disable IGMP report suppression. Disabling this feature will forward all IGMP reports to Multicast routers.

Note IGMP report suppression is supported only when the Multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The switch uses IGMP report suppression to forward only one IGMP report per Multicast router query to Multicast devices. When IGMP report suppression is enabled, the switch sends the first IGMP report from all hosts for a group to all Multicast routers. The switch does not send the remaining IGMP reports for the group to the Multicast routers. This feature prevents duplicate reports from being sent to the Multicast devices.

The switch always forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all Multicast routers, regardless of the Multicast router query also includes requests for IGMPv3 reports.

Step 3 Click **Apply**.

Step 4 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.
Multicast Router Ports Auto Learn	Select to enable Auto Learn of the Multicast router.
Query Robustness	Enter the robustness variable value to be used if this switch is the elected querier.
Query Interval	Enter the interval between the general queries to be used if this switch is the elected. querier.
Query Max Response Interval	Enter the delay used to calculate the maximum response code inserted into the periodic general queries.
Last Member Query Counter	Number of IGMP group-specific queries sent before the device assumes that there are no more members for the group, if the device is the elected querier.
Last Member Query Interval	Enter the maximum response delay to be used if the switch cannot read maximum response time value from group specific queries sent by the elected querier.
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.
IGMP Querier Status	Select to enable this feature. This feature is required if there's no Multicast router.
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.

Step 5 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.

MLD Snooping

To support selective IPv6 Multicast forwarding, bridge Multicast filtering must be enabled (in the Multicast Properties, on page 105), 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:

Step 1 Click **Multicast** > **MLD Snooping**.

Note MLD Snooping is only operational when Bridge Multicast Filtering is enabled and can be enabled here Multicast Properties, on page 105.

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
VLAN	Select the VLAN ID from the dropdown list.
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 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.

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.

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:

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:

- VLAN ID equals to—Defines the VLAN ID to query.
- IP Version equals to—Select either Version 4 or Version 6.
- IP Multicast Group Address equals to—Enter the IP Multicast group address to query.

Step 4 Click **Go**. The following fields are displayed for each Multicast group:

- VLAN—The VLAN ID.
- IP Multicast Group Address—The Multicast group IP address.
- Member Ports—The list of ports to where the corresponding Multicast stream is forwarded.
- Type—The group type is static or dynamic.

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:

Step 1 Click **Multicast** > **Multicast Router Port**.

Step 2 Enter the 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.
- 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

The Forward All page configures the ports and/or LAGs that receive Multicast streams from a specific VLAN.

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:

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.
- IP version – IPv4 or IPv6
- 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.

Maximum Multicast Groups

Use the Maximum Multicast Groups page to configure the maximum number of Multicast groups that are allowed on each interface and specify the action when the limit reaches.

To define the maximum number of IGMP and MLD groups on an interface:

Step 1 Click **Multicast** > **Maximum Multicast Groups**.

Step 2 Select the interface type (Port and LAG), and click **Go.**

Step 3 Select an interface and click **Edit**:

Step 4 Enter the following information:

- Interface—Select the port or LAG to be defined.
- IGMP Maximum Multicast Group—Enter the maximum number of IGMP groups that are allowed on the interface.
- IGMP Exceed Action—Denies or replaces the existing group with the new group for which the IGMP report was received when the limit is reached.
- MLD Maximum Multicast Group—Enter the maximum number of MLD groups that are allowed on the interface.
- MLD Exceed Action—Denies or replaces the existing group with the new group for which the MLD report was received when the limit is reached.

Step 5 Click **Apply**. The Running Configuration is updated.

Multicast Filtering

You can add a Multicast filter profile to permit or deny a range of Multicast groups be learned when the join groups match the profile IP group range, and assign the profile to an interface. The Multicast filter settings will be applied to the selected interface.

Multicast Filtering Profiles

A Multicast filter profile permits or denies a range of Multicast groups to be learned when the join group matches the filter profile IP group range.

To create a Multicast filter profile:

Step 1 Click **Multicast > Multicast Filtering > Profiles**.

Step 2 Select either Version 4 or Version 6 that the filter profile is applied to IPv4 or IPv6 Multicast traffic, and click Go.

Step 3 Click **Add**.

Step 4 Enter the following information:

- Profile Index—Enter the sequence number for the profile.
- IP Version—Select ether Version 4 or Version 6 to apply the filter profile to IPv4 or IPv6 Multicast traffic.
- Start Multicast Address—Enter the starting Multicast group address.
- End Multicast Address—Enter the ending Multicast group address.
- Action—Denies or permits Multicast frames when the join group matches.

Filter Settings

To assign a Multicast filter profile to an interface to deny or permit the Multicast group when the join group matches the filter profile:

Step 1 Click **Multicast** > **Multicast Filtering** > **Filter Settings**.

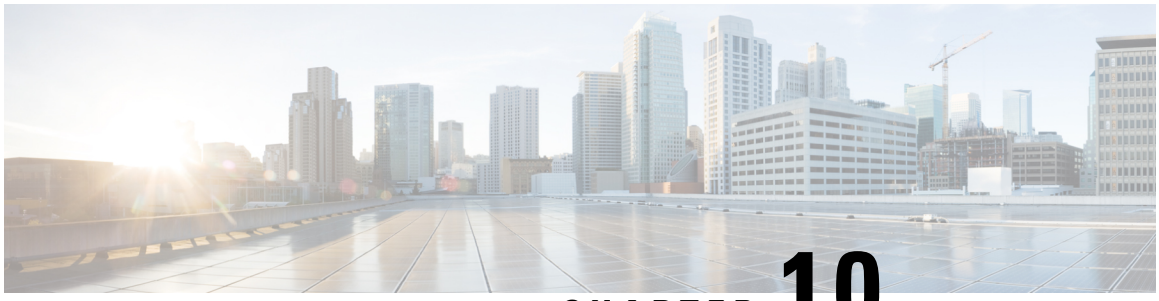
Step 2 Select the Interface Type equals to— To view either ports or LAGs.

Step 3 Select an interface and click **Edit**.

Step 4 Enter the following information:

- Interface—Select the port or LAG to be defined.
- Filter—Enable or disable filtering Multicast traffic on this interface.
- Filter Profile Index—If enabled, select the Multicast filter profile to be applied. The Multicast filter settings defined in the profile are applied to the interface.

Step 5 Click **Apply**. The Running Configuration file is updated.



CHAPTER 10

IP Config

This chapter contains the following sections:

- Management Interface, on page 115
- Domain Name System, on page 118

Management Interface

The switch has one IPv4 address and one IPv6 interface in the management VLAN. This IP address and the default gateway can be configured manually, or by DHCP. The static IP address and default gateway are configured on the IPv4 Interface and IPv6 Interface pages. The switch uses the default gateway, if configured, to communicate with devices that are not in the same IP subnet with the switch. By default, VLAN 1 is the management VLAN, but this can be modified. The switch can only be reached at the configured IP address through its management VLAN. The factory default setting of the IPv4 address configuration is DHCPv4. This means that the switch acts as a DHCPv4 client, and sends out a DHCPv4 request during boot up.

If the switch receives a DHCPv4 response from the DHCPv4 server with an IPv4 address, it sends Address Resolution Protocol (ARP) packets to confirm that the IP address is unique. If the ARP response shows that the IPv4 address is in use, the switch sends a DHCPDECLINE message to the offering DHCP server, and sends another DHCPDISCOVER packet that restarts the process.

If the switch does not receive a DHCPv4 response in 60 seconds, it continues to send DHCPDISCOVER queries, and adopts the default IPv4 address: 192.168.1.254/24.

IP address collisions occur when the same IP address is used in the same IP subnet by more than one device. Address collisions require administrative actions on the DHCP server and/or the devices that collide with the switch. When a VLAN is configured to use dynamic IPv4 addresses, the switch issues DHCPv4 requests until it is assigned an IPv4 address from a DHCPv4 server. Only the management VLAN can be configured with a static or dynamic IP address.

The IP address assignment rules for the switch are as follows:

- Unless the switch is configured with a static IP address, it issues DHCPv4 requests until a response is received from the DHCP server.
- The System LED on the front panel of the switch changes to solid green when a new unique IP address is received from the DHCP server. If a static IP address has been set, the System LED also changes to solid green. The System LED flashes when the switch is acquiring an IP address and is currently using the factory default IP address 192.168.1.254.

- The same rules apply when a client must renew the lease, prior to its expiration date, through a DHCPREQUEST message.
- With the factory default settings, when no statically-defined or DHCP acquired IP address is available, the default IP address is used. When the other IP addresses become available, the addresses are automatically used. The default IP address is always on the management VLAN.

To access and manage the switch by using the web-based interface, the switch management IP address must be defined and known. The default configuration of the switch is to use its factory default IP address of 192.168.1.254. The switch IP address can be manually configured.

IPv4 Interface

To manage the switch by using the web-based interface, the IPv4 management IP address must be defined and known. The switch IP address can be manually configured or automatically taken from a DHCP server.

To configure the IPv4 management IP address:

Step 1 Click **IP Configuration > Management Interface > IPv4 Interface**.

Step 2 Enter the following information:

- Management VLAN—Select the management VLAN used to access the switch through Telnet or the web-based interface. VLAN1 is the default management VLAN.
- IP Address Type—Select one of the following options:
  - Dynamic—Discovers the IP address using DHCP from the management VLAN.
  - Static—Manually defines a static IP address.

If a static IP address is used, enter the following fields:

- IP Address—Enter the management IP address of the switch. The default is 192.168.1.254.
- Mask—Enter the IP address mask or prefix length.
  - Network Mask—Select and enter the IP address mask.
  - Prefix Length—Select and enter the length of the IPv4 address prefix.
- Administrative Default Gateway—Select User Defined to manually enter the default gateway IP address, or select None to remove the selected default gateway IP address from the interface.
- Operational Default Gateway—Displays the current default gateway IP address.

Note If the switch is not configured with a default gateway, it cannot communicate with other devices that are not in the same IP subnet.

If a dynamic IP address is retrieved from the DHCP server, enter the following fields:

- Management VLAN—Select the management VLAN used to access the switch through Telnet or the web-based interface. VLAN1 is the default management VLAN.

- DHCP Force Auto Configuration—Check Enable to force the switch to perform auto configuration that will renew IP address from a DHCP server. The switch dynamic IP address can be renewed any time after it is assigned by a DHCP server. Note that depending on your DHCP server configuration, the switch may receive a new IP address after the renewal that requires setting the web-based interface to the new IP address.
- Auto Configuration via DHCP—Displays whether the DHCP Auto Configuration feature is enabled or disabled. You can configure this feature on the Administration > File Management > DHCP Auto Configuration page.

Step 3 Click **Apply**. The IPv4 interface settings are defined, and the Running Configuration is updated.

IPv6 Interface

The switch supports one IPv6 interface. In additional to the default link local and Multicast addresses, the switch also automatically adds global addresses to the interface based on the router advertisements that it receives. Each address must be a valid IPv6 address that is specified in hexadecimal format by using 16-bit values separated by colons.

To assign an IPv6 address to the IPv6 Interface:

Step 1 Click **IP Configuration > Management Interface > IPv6 Interface**.

Step 2 Check **Enable** next to IPv6 Address Auto Configuration field to automatically assign IPv6 addresses by the DHCPv6 server, or uncheck to disable this feature.

Step 3 Check **Enable** next to the DHCPv6 field to enable the DHCPv6 server, or uncheck to disable this feature.

Step 4 If you disable DHCPv6 and IPv6 Address Auto Configuration, manually enter the following fields:

- IPv6 Address—Enter the IPv6 address of the switch.
- Prefix Length—Enter the length of the global IPv6 prefix of the switch.
- IPv6 Gateway—Enter the link local IPv6 address of the default router.
- Link Local Address—Displays the IPv6 address of the local link.
- IPv6 Address Inuse—Displays the IPv6 address currently used by the switch.
- IPv6 Gateway Inuse—Displays the IPv6 gateway address currently used by the switch.

Step 5 To configure the interface as a DHCPv6 client so that the interface is able to receive information from the DHCPv6 server for DHCPv6 auto configuration feature, enter the DHCPv6 Client fields:

- Stateless—Check Enable to enable the interface as a stateless DHCPv6 client.
- Minimum Information Refresh Time—Select either Infinite (no refresh unless the server sends this option) or User Defined to manually set a value. 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.
- Information Refresh Time—Select either Infinite (no refresh unless the server sends this option) or User Defined to manually set a value. This value indicates how often the switch will refresh information received from the DHCPv6 server. If this option is not received from the server, the value entered here is used.

Step 6 Click **Apply**. The IPv6 interface settings are defined, and the Running Configuration is updated.

Domain Name System

The Domain Name System (DNS) translates domain names into IP addresses for the purpose of locating and addressing hosts. Asa 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:

Step 1 Click **IP Configuration** > **DNS** > **DNS Settings**.

Step 2 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.
- 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 non fully 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 3 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)

Step 4 Up to eight DNS servers can be defined. To add a DNS server, click **Add.**

Step 5 Enter the parameters.

- IP Version—Select Version 6 for IPv6 or Version 4 for IPv4.
- 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 6 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 118 and dynamic entries received from DHCPv4 and DHCPv6 servers.

To view the domain names that have been configured on the device, click **IP Configuration** > **DNS** > **Search List**.

The following fields are displayed for each DNS server configured on the device.

- Source—Source of the server's IP address (static or DHCPv4 or DHCPv6) 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.
- 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.

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.

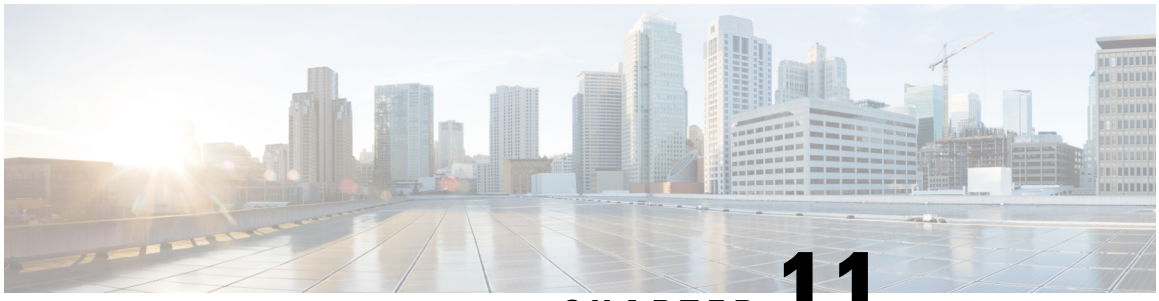
To add a host name and its IP address, complete the following:

Step 1 Click **IP Configuration** > **DNS** > **Host Mapping**.

Step 2 To add a host mapping, click **Add** and configure the following:

- IP Version—Select Version 6 for IPv6 or Version 4 for IPv4.
- 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 3 Click **Apply**. The settings are saved to the Running Configuration file.



CHAPTER 11

Security

This chapter contains the following sections:

- TACACS+, on page 121
- RADIUS Client, on page 122
- Management Access Method, on page 124
- Password Strength, on page 128
- Management Access Authentication, on page 128
- TCP/UDP Services, on page 129
- Storm Control , on page 131
- Port Security, on page 132
- 802.1X , on page 133
- Denial of Service, on page 137
- DHCP Snooping, on page 140
- IP Source Guard, on page 144
- ARP Inspection, on page 145
- Certificate Settings, on page 148

TACACS+

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 switch can act as a TACACS+ client that uses the TACACS+ server for the following services:

- Authentication—Provides authentication of administrators logging onto the switch 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.

The TACACS+ protocol ensures network integrity, through encrypted protocol exchanges between the device and the TACACS+ server

Some TACACS+ servers support a single connection that enables the device to receive all information in a single connection. If the TACACS+ server does not support this, the device reverts back to multiple connections.

Use the TACACS+ page to configure the TACACS+ servers and define the default parameters that are used for communicating with all TACACS+ servers. A user must be configured on the TACACS+ to have privilege level 15 to be granted permission to administer the switch.

To define default TACACS+ parameters and add a TACACS+ server:

Step 1 Click **Security** > **TACACS+**.

Step 2 Enter the default TACACS+ 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 TACACS+ Server page) the device uses the values in these fields.

- Timeout for Reply—Enter the amount of time in seconds that passes before the connection between the switch and the TACACS+ server times out. If a value is not entered for an individual server, the value is taken from this field.
- Key String—Enter the default key string in encrypted or plaintext form used for communicating with all TACACS+ servers. If you do not enter the default key string here, the key entered on the Add page must match the encryption key used by the TACACS+ server. If you enter the default key string here and a key string for an individual TACACS+ server, the key string configured for the individual TACACS+ server takes precedence.

Step 3 Click **Apply**. The TACACS+ default settings for the device are updated in the Running Configuration file.

Step 4 Enter the values in the fields for each TACACS+ server. To use the default values entered in the RADIUS page, select **Use Default**.

- Server Definition—Select whether to specify the TACACS+ server by IP address or name.
- IP Version—Select the version of the IP address of the TACACS+ server.
- Server IP Address/Name—Enter the TACACS+ 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 TACACS+ server first. Zero is the highest priority
- Key String—Enter the default key string in encrypted or plaintext form used for communicating with all TACACS+ servers. If you do not enter the default key string here, the key entered on the Add page must match the encryption key used by the TACACS+ server. If you enter the default key string here and a key string for an individual TACACS+ server, the key string configured for the individual TACACS+ server takes precedence.

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

Step 6 To display sensitive data in plaintext form on the 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:

Step 1 Click **Security > RADIUS Client**.

Step 2 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.
- 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.

Step 3 Click **Apply**. The RADIUS default settings for the device are updated in the Running Configuration file.

Step 4 To add a RADIUS server, click **Add**.

Step 5 Enter the values in the fields for each RADIUS server. To use the default values entered in the RADIUS page, select **Use Default**.

- 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.
- 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
- 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.
- 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 6 Click **Apply**. The RADIUS server definition is added to the Running Configuration file of the device.

Step 7 To display sensitive data in plaintext form on the page, click **Display Sensitive Data As Plaintext**.

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 Profile

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.

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.

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 displays if you selected any other access profile, warning you that, depending on the selected access profile, you might be disconnected from the web-based configuration utility.

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 255 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:

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.

Password Strength

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, (**Password Complexity Settings** are enabled in the Password Strength page), you're prompted to create another password.

To define password complexity rules:

Step 1 Click **Security** > **Password Strength**.

Step 2 Enter the following parameters for passwords:

- Password Aging—If selected, the user is prompted to change the password when the Password Aging Time expires.
- Password Aging Time—Enter the number of days that can elapse before the user is prompted to change the password.

Step 3 The following parameters may be configured:

- Minimal Password Length—Enter the minimal number of characters required for passwords.
- Allowed Character Repetition—Enter the number of times that a character can be repeated.
- Minimal Number of Character Classes—Enter the number of character classes which must be present in a password. Character classes are lower case (1), upper case (2), digits (3), and symbols or special characters (4).

Step 4 Click **Apply**. The password settings are written to the Running Configuration file.

The following requirements are always enforced:

- New password is different from the current password
- New Password does not repeat or reverse the users name
- New Password does not repeat or reverse the manufacturers name

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:

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 cisco-avpair = shell:priv-lvl=15.
- 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.

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:

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.
  - ESTABLISHED—The socket has an established connection.
  - SYN_SENT—The socket is actively attempting to establish a connection.
  - SYN_RECV—A connection request has been received from the network.
  - FIN_WAIT1—The socket is closed, and the connection is shutting down.
  - FIN_WAIT2—The connection is closed, and the socket is waiting for a shutdown from the remote end.
  - TIME_WAIT—The socket is waiting after close to handle packets still in the network
  - CLOSED—The socket is not being used.
  - CLOSE_WAIT—The remote end has shut down, waiting for the socket to close.
  - LAST_ACK—The remote end has shut down, and the socket is closed. Waiting for acknowledgment
  - LISTEN—The socket is listening for incoming connections.
  - CLOSING—Both sockets are shut down but we still do not have all our data sent.
  - UNKNOWN—The state of the socket is unknown.

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.

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.

To define Storm Control, follow these steps:

Step 1 Click **Security** > **Storm Control**.

Step 2 Configure the following parameters.

- Frame Configuration—Select Included (including preamble and IFG 20Bytes) to count the Broadcast, unknown Multicast, or unknown Unicast frames, or select Excluded (excluding preamble and IFG 20Bytes) to not count the Broadcast, unknown Multicast, or unknown Unicast frames
- Storm Control Rate Threshold Mode—Select the mode of the rate threshold: Packets per second or Kbits/sec.

Step 3 Click **Apply**. The storm control parameters are defined, and the Running Configuration is updated

Step 4 Select a port and click **Edit.**

Step 5 Enter the parameters.

- Interface—Select the port for which storm control is enabled.
- Storm Control—Select to enable Storm Control on selected port.
- Unknown Unicast—Select to enable Storm Control for Unicast packets.
- Storm Control 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.
- Unknown Multicast—Select to enable Storm Control for Multicast packets.
- Storm Control 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.
- Broadcast—Select to enable Storm Control for Broadcast packets.
- Storm Control 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.
- Action—Select to shut down a port when a storm occurs on the port. If this isn’t selected extra traffic is discarded.

Step 6 Click **Apply**. Storm control is modified, and the Running Configuration file is updated.

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 two 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.

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.
- Frame is discarded and a SYSLOG message is generated.
- 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:

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.
- 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
  - Discard and Log—Discards packets from any unlearned source, shuts down the interface, logs the events, and sends traps to the specified trap receivers
  - 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 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

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 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:

Step 1 Click **Security > 802.1X > Properties**.

Step 2 Enter the parameters.

- Port-Based Authentication—Enable or disable port-based authentication.
- 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.

Step 3 Click **Apply**. The 802.1X properties are written to the Running Configuration file.

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:

Step 1 Click **Security** > **802.1X** > **Port Authentication**.

This page displays authentication settings for all ports.

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

Step 3 Enter the parameters.

- Interface—Select a port.
- Administrative Port Control—Select the Administrative Port Authorization state. The options are:
  - Disable—Disable 802.1X
  - 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. The options are:
  - Disable—Ignore the VLAN authorization result and keep original VLAN of host.
  - Reject—If get VLAN authorized information, just use it. However, if there is no VLAN authorized information, reject the host and make it unauthorized
  - Static—If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host

Note If there is VLAN authorized information from RADIUS, but the VLAN is not administrative created on DUT, the VLAN will be created automatically

Tip For the Dynamic VLAN Assignment feature to work, the switch requires the following VLAN attributes to be sent by the RADIUS server (as defined in RFC 3580):

- [64] Tunnel-Type = VLAN (type 13)
- [65] Tunnel-Medium-Type = 802 (type 6)
- [81] Tunnel-Private-Group-Id = VLAN ID

- Guest VLAN—Select to enable using a guest VLAN for unauthorized ports.
- 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.

- 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.
- 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.

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:

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.

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
- MAC Address—Displays the supplicant MAC address.

Denial of Service

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:

Step 1 Click **Security** > **Denial of Service Prevention** > **Security Suite Settings**.

CPU Protection Mechanism: Enabled indicates that SCT is enabled.

Step 2 Click **Details** to view CPU resource utilization information.

Step 3 Click **Edit** beside TCP SYN Protection to set the feature.

Step 4 In the **Denial of Service Protection** area, enable one or more of the following DoS protection options and specify the threshold if necessary:

- DA Equals SA
- ICMP Frag Packets

- ICMP Ping Maximum Length
- IPv6 Minimum Frag Length
- Land
- Null Scan
- POD
- Smurf Netmask
- TCP Source Port Less 1024
- TCP Blat
- TCP Frag-Off Minimum check
- TCP Herder Minimum Length
- UDP Blat
- XMA

Step 5 Click **Apply**. The Denial of Service prevention Security Suite settings are written to the Running Configuration file.

Interface Settings

Use the Interface Settings to enable DoS protection and IP gratuitous ARP protection on specific ports. The DoS protection feature enabled in security suite will take effect on DoS protection enabled ports.

To enable DoS protection and IP gratuitous ARP protection on a port:

Step 1 Click **Security > Denial of Service Prevention > Interface Settings**.

The Interface Settings Table displays the following information:

- Interface—Shows the port ID
- Denial of Service Protection—Shows whether the DoS Protection feature is enabled or disabled on the port.
- IP Gratuitous ARPs Protection—Check Enable to enable the IP gratuitous ARP protection feature on the port, or uncheck to disable this feature on the port.

Step 2 To edit the DoS settings for a port, select the desired port, and click **Edit**.

Step 3 Enter the following information:

- Interface—Select the port to be configured.
- Denial of Service Protection—Check **Enable** to enable the DoS Protection feature on the port, or uncheck to disable this feature on the port.
- IP Gratuitous ARPs Protection—Check **Enable** to enable the IP gratuitous ARP protection feature on the port, or uncheck to disable this feature on the port.

Step 4 Click **Apply**. The DoS protection and IP gratuitous ARP protection are enabled or disabled on the port, and the Running Configuration is updated.

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:

Step 1 Click **Security** > **Denial of Service Prevention** > **SYN Protection**.

Step 2 Enter the parameters.

- Block SYN-RST Packets-Select to enable the feature. All TCP packets with both SYN and RST flags are dropped on all ports.
- 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 or SYN-RST attack identified by the system and the system action.

DHCP Snooping

DHCP Snooping provides network security by filtering untrusted DHCP messages and by building and by maintaining a DHCP Snooping binding database (table). DHCP Snooping acts as a firewall between untrusted hosts and DHCP servers. DHCP Snooping differentiates between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

DHCP Snooping Properties

Use the Properties page to enable DHCP Snooping on the switch and define general DHCP Snooping parameters. To define general DHCP Snooping properties:

Step 1 Click **Security > DHCP Snooping > Properties**.

Step 2 Enter the following information:

- DHCP Snooping Status—Check **Enable** to enable DHCP Snooping on the switch, or uncheck to disable this feature. By default, DHCP Snooping is disabled.
- DHCP Packet Validation—Check **Enable** to enable verifying (on an untrusted port) 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), uncheck to disable this feature. By default, it is disabled.
- Option 82 Status—Check **Enable** to enable global Option 82 insert on the switch, or uncheck to disable this feature.
- Remote ID—If Option 82 is enabled, select User Defined to manually enter the format remote ID, or select Use Default to use the default value.
- Backup Database Type—Set the type of backup DHCP Snooping database agent. The options are:
  - None—Disables DHCP Snooping database agent.
  - Flash—Saves DHCP Snooping binding database in the switch NVRAM.
  - TFTP—Saves DHCP Snooping binding database on a TFTP server.
- File Name—When TFTP is selected, enter the file name of the DHCP Snooping settings that will be written to the TFTP server.
- Server IP Address—When TFTP is selected, enter the IP address or host name of the remote TFTP server.
- Write Delay—Enter the duration in seconds for which the transfer should be delayed after the DHCP Snooping binding database changes. The default is 300 seconds. The range is from 15 to 86400 seconds.
- Timeout—Enter the value in seconds when to stop the database transfer process after the DHCP Snooping binding database changes. The default is 300 seconds. The range is from 0 to 86400. Use 0 to define an Infinite duration

Step 3 Click **Apply**. The DHCP Snooping properties are defined, and the Running Configuration is updated.

DHCP Snooping VLAN Settings

Use the VLAN Settings page to enable DHCP Snooping on VLANs. To enable DHCP Snooping on a VLAN, ensure that DHCP Snooping is globally enabled on the switch.

To define DHCP Snooping on VLANs, complete the following steps:

Step 1 Click **Security** > **DHCP Snooping** > **VLAN Settings**.

Step 2 Select the VLANs from the Available VLANs column and add them to the Enabled VLANs column.

Step 3 Click **Apply**. DHCP Snooping is enabled on the selected VLANs, the Running Configuration is updated

DHCP Snooping Interface Settings

Use the Interface Settings page to define the DHCP Snooping trusted interfaces. The switch transfers all DHCP requests to trusted interfaces. To define DHCP Snooping trusted interfaces:

Step 1 Click **Security** > **DHCP Snooping** > **Interface Settings**.

Step 2 Select the interface type (Port or LAG), and click **Go**.

Step 3 Select an interface and click **Edit**.

Step 4 Enter the following information:

- Trusted Interface—Select to trust or not trust the selected interface.

Note Configure the ports that are connected to a DHCP server or to other switches or routers as trusted ports. Configure the ports that are connected to DHCP clients as untrusted ports.

- Rate Limit (pps)—Check to limit the rate on the interface. If rate limit is enabled, enter the maximum number of rate that can be allowed on the interface.

Step 5 Click **Apply**. The DHCP Snooping trusted interface settings are defined, and the Running Configuration is updated.

Binding Database

Use the Binding Database page to query the DHCP Snooping binding database. To query addresses that are bound to the DHCP Snooping database:

Step 1 Click **Security** > **DHCP Snooping** > **Binding Database**.

Step 2 Define any of the following fields as a query filter:

- VLAN ID—Indicates the VLANs recorded in the DHCP database.

- MAC Address—Indicates the MAC addresses recorded in the DHCP database.
- IP Address—Indicates the IP addresses recorded in the DHCP database.
- Interface—Contains the interface by which the DHCP database can be queried.

Step 3 Click **Go**. These appear in the Binding Database table:

- VLAN ID—VLAN ID to which the IP address is attached in the DHCP Snooping Database.
- MAC Address—MAC address found during the query.
- IP Address—IP address found during the query.
- Interface—Interface connected to the address found during the query.
- Type—IP address binding type. The possible values are:
  - Static—Indicates the IP address is static.
  - Dynamic—Indicates the IP address is defined as a dynamic address in the DHCP database.
- Lease Time—The amount of time that the DHCP Snooping entry is active.

Addresses whose lease times are expired are deleted from the database.

DHCP Snooping Statistics

To view DHCP Snooping statistics:

Step 1 Click **Security > DHCP Snooping > Statistics**.

Step 2 Select the interface type (Port or LAG), click **Go**.

The following DHCP Snooping statistical information is displayed:

- Port—Port identifier or LAG identifier.
- Forward—Total number of forwarded packets.
- Chaddr Check Dropped—Total number of packets that are dropped by Chaddr check.
- Untrust Port Dropped—Total number of packets that are dropped by untrusted ports.
- Untrust Port with Option 82 Dropped—Total number of packets that are dropped by untrusted ports that enable Option 82.
- Invalid Drop—Total number of packets that are dropped due to invalid.

Step 3 Click **Refresh** to refresh the data in the table, or click Clear to clear all data in the table.

Option82 Port Settings

Use the Option82 Port Settings page to accept DHCP packets with Option 82 information that are received on the untrusted interfaces. To define the action for packets received on an untrusted interface, complete the following:

Step 1 Click **Security > DHCP Snooping > Option82 Port Settings**.

Step 2 Select the interface type (Port or LAG), click **Go**.

Step 3 Select an interface and click **Edit**.

Step 4 Enter the following information:

- Interface—Select the port or LAG to be defined.
- Allow Untrusted—Select one of the following actions when the untrusted port receives DHCP packets:
  - Keep—Keeps DHCP packets with Option 82 information.
  - Drop—Drops DHCP packets with Option 82 information.
  - Replace—Replaces DHCP packets with Option 82 information.

Step 5 Click **Apply**. The Running Configuration is updated.

Option82 Port CID Settings

Use the Option82 Port CID Settings page to configure the Option 82 circuit-ID sub-option. To configure the Option 82 circuit-ID sub-option, complete the following:

Step 1 Click **Security > DHCP Snooping > Option82 Port CID Settings.**

Step 2 Click **Add**.

Step 3 Enter the following information:

- Interface—Select a port or a LAG.
- VLAN Status—Check Enable to use circuit ID on a specific VLAN, or uncheck to use circuit ID on all VLANs.
- VLAN ID—Select the VLAN ID.
- Circuit ID—Enter the circuit ID, using from 1 to 63 ASCII characters (no spaces). When the Option 82 feature is enabled, the default circuit-ID sub-option is the switch VLAN and port identifier, in the format of vlan-modport.

Step 4 Click **Apply**. The Running Configuration is updated.

IP Source Guard

IP Source Guard restricts the client IP traffic to those source IP addresses configured in the IP Source binding database. For example, IP Source Guard can help prevent traffic attacks caused when a host tries to use the IP address of its neighbor.

Interface Settings

Use the Interface Settings page to enable IP Source Guard on the interfaces. To enable IP Source Guard on an interface, complete the following steps:

Step 1 Click **Security** > **IP Source Guard** > **Interface Settings.**

Step 2 Select the interface type (Port or LAG), click **Go**.

Step 3 Select an interface, and click **Edit**.

Step 4 Enter the following information:

- Interface—Select a port or LAG.
- IP Source Guard—Check **Enable** to enable IP Source Guard on the interface, or uncheck to disable this feature on the interface.
- Verify Source—Select the type of source traffic to be verified. It can be IP or MAC and IP.
- Maximum Entry—Enter the maximum number of IP source binding rules. The range is 0 to 50, and 0 means no limit.

Step 5 Click **Apply**. The IP Source Guard Interface settings are defined, and the Running Configuration is updated.

IP Source Guard Binding Database

Use the Binding Database page to query and view information about inactive addresses recorded in the IP Source Guard database. To query the IP Source Guard database and/or define an IP source binding rule:

Step 1 Click **Security > IP Source Guard > Binding Database.**

Step 2 Define the preferred filter for searching the IP Source Guard database:

- VLAN ID—Queries the database by VLAN ID.
- MAC Address—Queries the database by MAC address.
- IP Address—Queries the database by IP address.
- Interface—Queries the database by Interface name.

Step 3 Click **Go**. These appear in the Binding Database table:

- VLAN ID—VLAN with which the IP address is associated.

- MAC Address—MAC address of the interface.
- IP Address—IP address of the interface.
- Interface—Interface name.
- Type—Type of the IP address. The possible values are:
  - Dynamic—Indicates the IP address is dynamically learned.
  - Static—Indicates the IP address is a static IP address.
- Lease Time—The amount of time that the IP address is active. IP addresses whose lease times are expired are deleted from the database.

Step 4 Click **Add** to add an IP source binding rule.

Step 5 Enter the following information:

- Interface—Select an interface.
- VLAN ID—Select a VLAN with which the address is associated.
- MAC Address—Enter the MAC address of the source traffic.
- IP Address—Enter the IP address of the source traffic.

Step 6 Click **Apply**. The IP source binding rule is defined, and the Running Configuration is updated.

ARP Inspection

Dynamic Address Resolution Protocol (ARP) is a TCP/IP protocol for translating IP addresses into MAC addresses.

ARP Cache Poisoning

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 situation 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.

How ARP Inspection Prevents Cache Poisoning

The ARP inspection feature relates to interfaces as either trusted or untrusted (see Security > ARP Inspection > Interface Settings page). Interfaces are classified by the user as follows:

- Trusted—Packets are not inspected.
- Untrusted—Packets are inspected as described below.

ARP inspection is performed only on untrusted interfaces. ARP packets that are received on the trusted interface are simply forwarded.

Upon packet arrival on untrusted interfaces the following logic is implemented:

- Search the ARP access control rules for the packet's IP/MAC addresses. If the IP address is found and the MAC address in the list matches the packet's MAC address, then the packet is valid
- If the packet's IP address was not found, and DHCP Snooping is enabled for the packet's VLAN, search the DHCP Snooping Binding database for the packet's <VLAN - IP address> pair. If the <VLAN - IP address> pair was found, and the MAC address and the interface in the database match the packet's MAC address and ingress interface, the packet is valid.
- If the packet's IP address was not found in the ARP access control rules or in the DHCP Snooping Binding database the packet is invalid and is dropped. A SYSLOG message is generated.
- If a packet is valid, it is forwarded and the ARP cache is updated.

If the ARP Packet Validation option is selected (on the Properties page), the following additional validation checks are performed:

- Source MAC Address—Compares the packet's source MAC address in the Ethernet header against the sender's MAC address in the ARP request. This check is performed on both ARP requests and responses.
- Destination MAC Address—Compares the packet's destination MAC address. This check is performed for ARP responses.
- IP Address—Compares the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP Multicast addresses.

Packets with invalid ARP Inspection bindings are logged and dropped.

Interaction Between ARP Inspection and DHCP Snooping

If DHCP Snooping is enabled, ARP Inspection uses the DHCP Snooping Binding database in addition to the ARP access control rules. If DHCP Snooping is not enabled, only the ARP access control rules are used.

Table 2: ARP Default

Option	Default State
Dynamic ARP Inspection	Disabled
ARP Packet Validation	Disabled
ARP Inspection Enabled on VLAN	Disabled
Log Buffer Interval	SYSLOG message generation for dropped packets is enabled at 10 seconds interval.

ARP Properties

Use the Properties page to enable dynamic ARP Inspection on the switch and set ARP packet validation parameters. To define ARP Inspection properties complete the following:

Step 1 Click **Security > ARP Inspection > Properties** .

Step 2 Enter the following information:

- ARP Inspection Status—Check **Enable** to enable ARP Inspection on the switch, or uncheck to disable this feature. By default, ARP Inspection is disabled.
- ARP Packet Validation—Defines the following ARP Inspection validation properties:
  - Source MAC Address—Check **Enable** to validate the source MAC addresses in ARP requests and replies.
  - Destination MAC Address—Check **Enable** to validate the destination MAC addresses in ARP replies.
  - IP Address—Check **Enable** to validate the IP addresses in ARP requests and replies.
  - Allow all-zeros IP—If IP address validation is enabled, check **Enable** to allow 0.0.0.0 the IP address.

Step 3 Click **Apply**. The ARP Inspection properties are defined, and the Running Configuration is updated.

ARP Inspection Interface Settings

Use the Interface Settings page to define trusted and untrusted interfaces. These settings are independent to the trusted interface settings defined for DHCP Snooping. ARP Inspection is enabled only on untrusted interfaces. To change the ARP trusted status of an interface:

Step 1 Click **Security** > **ARP Inspection** > **Interface Settings**.

Step 2 Select the interface type (Port or LAG), and click **Go**.

Step 3 Select an interface, and click **Edit**.

Step 4 Enter the following information:

- Interface—Select a port or LAG on which ARP Inspection trust mode can be enabled.
- Trusted Interface—Click Yes to enable ARP Inspection trust mode on the interface, or click No to disable ARP Inspection trust mode on the interface
  - If enabled, the port or LAG is a trusted interface, and ARP inspection is not performed on the ARP requests or replies sent to or from the interface.
  - If disabled, the port or LAG is not a trusted interface, and ARP inspection is performed on the ARP requests or replies sent to or from the interface. By default, it is disabled.
- Rate Limit (pps)—Enter the maximum rate that is allowed on the interface. The range is 1 to 50 pps and the default is 15.

Step 5 Click **Apply**. The ARP Inspection trusted interfaces are defined, and the Running Configuration is updated.

ARP Inspection Statistics

The Statistics page displays the statistical information for ARP Inspection. To view ARP Inspection statistics:

Step 1 Click **Security > ARP Inspection > Statistics**.

- VLAN ID—Identifier of the VLAN.
- Forward—Total number of ARP packets forwarded by the VLAN.
- Source MAC Failures—Total number of ARP packets that include wrong source MAC addresses.
- Destination MAC Failures—Total number of ARP packets that include wrong destination MAC addresses.
- Source IP Address Validation Failures—Total number of ARP packets that the source IP address validation fails.
- Destination IP Address Validation Failures—Total number of ARP packets that the destination IP address validation fails.
- IP-MAC Mismatch Failures—Total number of ARP packets that the IP address does not match the MAC address.

Step 2 Click **Refresh** to refresh the data in the table, or click Clear to clear all ARP Inspection statistics.

ARP Inspection VLAN Settings

Use the VLAN Settings page to enable ARP Inspection on VLANs. In the Enabled VLAN table, users assign static ARP Inspection lists to enabled VLANs. When a packet passes through an untrusted interface that is enabled for ARP Inspection, the switch performs the following checks in order:

- Determines if the packet's IP address and MAC address exist in the static ARP Inspection list. If the addresses match, the packet passes through the interface.
- If the switch does not find a matching IP address, but DHCP Snooping is enabled on the VLAN, the switch checks the DHCP Snooping database for the IP address-VLAN match. If the entry exists in the DHCP Snooping database, the packet passes through the interface.
- If the packet's IP address is not listed in the ARP Inspection list or the DHCP Snooping database, the switch rejects the packet.

To define ARP Inspection on VLANs, complete the following steps:

Step 1 Click **Security > ARP Inspection > VLAN Settings**.

Step 2 Select the VLANs from the Available VLANs column and add them to the Enabled VLANs column.

Step 3 Click **Apply**. ARP Inspection settings are applied on the selected VLANs, and the Running Configuration is updated.

Certificate Settings

The Cisco Business Dashboard Agent (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 longerwanted
- Statically add certificates to device configurationfile
- Manage a revocation list of untrustedcertificates

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 embedded certificate is installed by default. The 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)
- 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 Certificate

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 - A string that is used to identify the certificate
- Owner - The application name that installed the certificate (for example, PNP)
- The certificate itself in PEM format.

Considerations

- Up to 128 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:

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 Owner —Enter the owner 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 Certificate 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:

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:

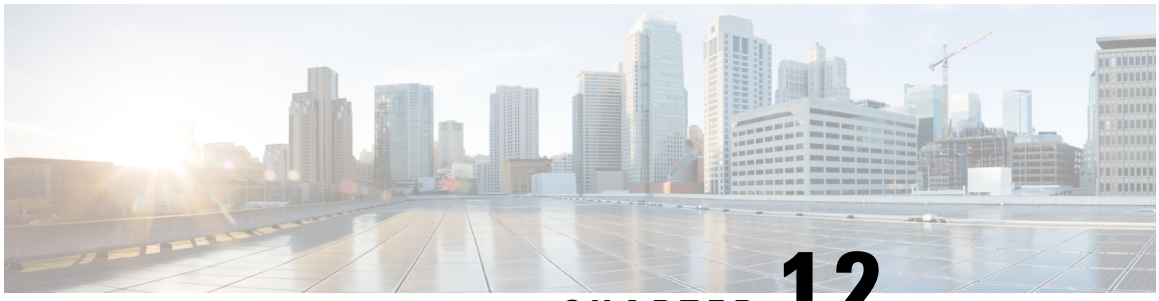
- Issuer—The string identifying the issuer (for example: "C=US, O=MyTrustOrg, CN=MyCommonName") (1-160 chars).
- Serial Number—The serial number of the revoked certificate. This is a string of hexadecimal pairs (length 2-32).

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**. Next, click **Apply** to apply the new settings.



CHAPTER 12

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 153
- MAC-based ACE, on page 154
- IPv4-based ACL, on page 155
- IPv4-Based ACE, on page 155
- IPv6-Based ACL, on page 158
- IPv6-Based ACE, on page 158
- ACL Binding , on page 161

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:

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:

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.
- 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 mask 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's 0 and don't match on the bits where there are 1's). You need to translate the 1's to a hexadecimal value and you write 0 for every four zeros. 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.
- Ether type—Enter the frame Ether type 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:

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

To add rules (ACEs) to an IPv4-based ACL, follow these steps:

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.

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 • 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. • 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 • RSVP—ReSerVation Protocol • IPV6:ICMP—Internet Control Message Protocol • OSPF—Open Shortest Path First • PIM—Protocol Independent Multicast • L2TP—Layer 2 Tunneling 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.
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.

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:

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:

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.
Protocol	Select to create an ACE based on a specific protocol from the following options: • 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. • ICMPv6—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.
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

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:

Step 1 Click **Access Control** > **ACL Binding**.

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:

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).

Step 4 To unbind all ACLs from an interface, select the interface, and click **Clear**.

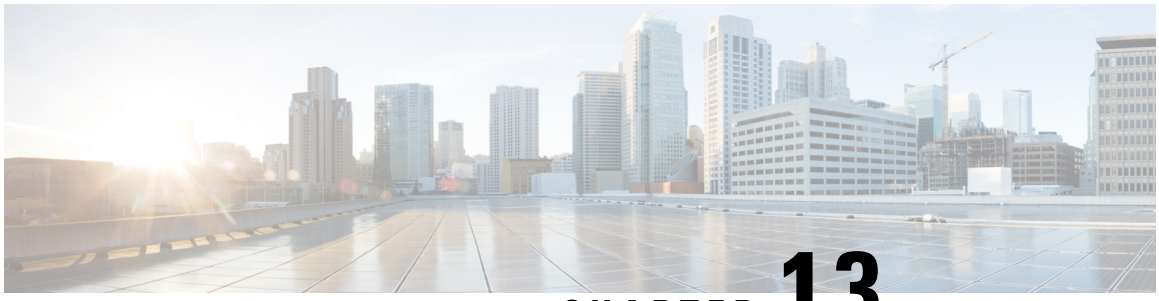
Step 5 Select an interface, and click **Edit**.

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.

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 13

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:

- QoS General, on page 163
- QoS Basic Mode, on page 172
- QoS Advanced Mode, on page 174

QoS 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:

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**.

Queue

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:

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)	Notes
0	2	Background
1	1	Best Effort
2	3	Excellent Effort
3	4	Critical Application - LVS phone SIP
4	5	Video
5	6	Voice - Cisco IP phone default
6	7	Interwork Control LVS phone RTP
7	8	Network Control

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:

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.

IP Precedence to a Queue

The IP Precedence to Queue page maps IP Precedence priorities to egress queues. The IP Precedence to Queue Table determines the egress queues of the incoming packets based on the IP Precedence priority.

The following table describes the default mapping when there are 8 queues:

IP Precedence Values (0-7,7 being the highest)	Queue (8 queues 1-8,8 is the highest priority)	Notes
0	1	Background
1	2	Best Effort
2	3	Excellent Effort
3	4	Critical Application - LVS phone SIP
4	5	Video
5	6	Voice - Cisco IP phone default
6	7	Interwork Control LVS phone RTP
7	8	Network Control

By changing the IP Precedence to Queue mapping (IP Precedence to Queue) and the Queue schedule method and bandwidth allocation, it's possible to achieve the desired quality of service in a network.

The IP Precedence to Queue mapping is applicable to IP packets if:

- The device is in QoS Basic mode and IP Precedence is the trusted mode.
- The device is in QoS Advanced mode and the packets belongs to flows that are IP Precedence trusted.

To map IP Precedence values to egress queues, follow these steps:

Step 1 Click **Quality of Service > General > IP Precedence to Queue**.

Step 2 Enter the parameters.

- IP Precedence—Displays the IP Precedence priority 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 IP Precedence priority is mapped.

Step 3 For each IP Precedence priority, select the Output Queue to which it is mapped.

Step 4 Click **Apply, Cancel or Restore Defaults**. IP Precedence 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 8 is highest:

DSCP	63	55	47	39	31	23	15	7
Queue	8	7	6	5	4	3	2	1
DSCP	62	54	46	38	30	22	14	6
Queue	8	7	6	5	4	3	2	1
DSCP	61	53	45	37	29	21	13	5
Queue	8	7	6	5	4	3	2	1
DSCP	60	52	44	36	28	20	12	4
Queue	8	7	6	5	4	3	2	1
DSCP	59	51	43	35	27	19	11	3
Queue	8	7	6	5	4	3	2	1
DSCP	58	50	42	34	26	18	10	2

Queue	8	7	6	5	4	3	2	1
DSCP	57	49	41	33	25	17	9	1
Queue	8	7	6	5	4	3	2	1
DSCP	56	48	40	32	24	16	8	0
Queue	8	7	6	5	4	3	2	1

To map DSCP to queues, follow these steps:

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.

Queue to CoS_802_1p

Use the Queues to CoS/802.1p page to remark the CoS/802.1p priority for egress traffic from each queue.

To map queues to CoS values, follow these steps:

Step 1 Click **Quality of Service > General > Queues to CoS/802.1p**.

Step 2 Enter the parameters.

- Output Queue—Display the egress queue to which the 802.1p priority is mapped.
- 802.1p—Select the 802.1p priority tag values to be remarked.

Step 3 For each output queue, select the CoS/802.1p priority to which egress traffic from the queue is remarked

Step 4 Click **Apply, Cancel** or **Restore Defaults**. Queues to 801.1p priority values are remarked, and the Running Configuration file is updated, the changes that entered are canceled, or previously defined values are restored.

Queue to IP Precedence

Use the Queues to IP Precedence page to remark the IP Precedence value for egress traffic from each queue.

To map queues to IP Precedence values, follow these steps:

Step 1 Click **Quality of Service > General > Queues to IP Precedence.**

Step 2 Enter the parameters.

- Output Queue—Display the egress queue to which the IP Precedence value is mapped.
- IP Precedence—Select the IP Precedence values to be remarked.

Step 3 For each output queue, select the IP Precedence value to which egress traffic from the queue is remarked.

Step 4 Click **Apply, Cancel or Restore Defaults**. Queues to IP Precedence priority values are remarked, and the Running Configuration file is updated, the changes that entered are canceled, or previously defined values are restored.

Queue to DSCP

Use the Queues to DSCP page to remark the DSCP value for egress traffic from each queue.

To map queues to DSCP values, follow these steps:

Step 1 Click **Quality of Service > General > Queues to DSCP**.

Step 2 Enter the parameters.

- Output Queue—Display the egress queue to which the DSCP value is mapped.
- DSCP—Select the DSCP values to be remarked.

Step 3 For each output queue, select the DSCP value to which egress traffic from the queue is remarked.

Step 4 Click **Apply, Cancel** or **Restore Defaults**. Queues to DSCP priority values are remarked, and the Running Configuration file is updated, the changes that entered are canceled, or previously defined values are restored.

Remark Interface

Use the Remark Interface Settings page to remark the CoS/802.1p priority, IP precedence, and DSCP value for egress traffic on a port. The CoS/802.1p priority and IP or the CoS/802.1p priority and DSCP value can be remarked simultaneously, but the DSCP value and IP cannot be remarked simultaneously

To remark egress traffic on an interface:

Step 1 Click **Quality of Service > General > Remark Interface Settings**.

Step 2 Select an interface type (Port or LAG), and click **Go**.

Step 3 Select a Port/LAG, and click **Edit**.

Step 4 Enter the parameters.

- Interface—Select the port or LAG to be defined.
- Remark CoS—Check Enable to remark the CoS/802.1p priority for egress traffic on this port or LAG.
- Remark IP Precedence—Check Enable to remark the IP precedence for egress traffic on this port or LAG.
- Remark DSCP—Check Enable to remark the DSCP value for egress traffic on this port or LAG.

Step 5 Click **Apply**. The Running Configuration is updated

Bandwidth

The Bandwidth page displays bandwidth information for each interface. To view the bandwidth information, complete the following steps:

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.
- **Egress Shaping Rates**:
  - Status—Displays whether Egress Shaping Rates is enabled.
  - CIR (KBits/sec)—Displays the maximum bandwidth for the egress interface.

Step 2 Select an interface, and click **Edit**.

Step 3 Select the Port 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).
Egress Shaping Rate	Select to enable egress shaping on the interface.
Committed Information Rate (CIR)	Enter the maximum bandwidth for the egress interface.

Step 5 Click **Apply**. The bandwidth settings are written to the Running Configuration file.

Egress Shaping per Queue

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:

Step 1 Click **Quality of Service** > **General** > **Egress Shaping per Queue**.

The Egress Shaping Per Queue page displays the rate limit (CIR) for each queue.

Step 2 Select an interface type (Port), and click **Go**.

Step 3 Select a Port, 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.

Step 6 Click **Apply**. The bandwidth settings are written to the Running Configuration file.

VLAN Ingress Rate Limit

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.

To define the VLAN ingress rate limit, complete the following steps:

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.

Step 4 Click **Apply**. The VLAN rate limit is added, and the Running Configuration file is updated.

VLAN Port Ingress Rate Limit

Rate limiting per VLAN port, performed on the VLAN Port Ingress Rate Limit page, enables traffic limiting on the ports that are bound to a specific VLAN. When VLAN port ingress rate limiting is configured, it limits aggregate traffic from the specified ports on the switch.

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 port rate limiting, and the rate limits conflict, the QoS rate limits take precedence.

To define the VLAN Port ingress rate limit, complete the following steps:

Step 1 Click Quality of Service > General > VLAN Port Ingress Rate Limit.

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
- Interface — Enter an interface or a range of interfaces. The interfaces must be bound to the selected VLAN.

Step 4 Click **Apply**. The VLAN Port rate limit is added, and the Running Configuration file is updated

TCP Congestion Avoidance

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:

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:

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 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:

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.
- 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:

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.

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:

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 is Or. This indicates the relationship between the ACLs. The Class Map is then the result of the three ACLs combined with 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 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:

- A maximum allowed rate, called a Committed Information Rate (CIR), measured in Kbps.
- 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, 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:

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 170.
- 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.

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.

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:

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:

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.
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.
Exceed Action	Select the action assigned to incoming packets exceeding the CIR. The options are: • Drop—Packets exceeding the defined CIR value are dropped.

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. 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:

Step 1 Click **Quality of Service** > **QoS Advanced Mode** > **Policy Binding**.

Step 2 Select an Interface Type if required.

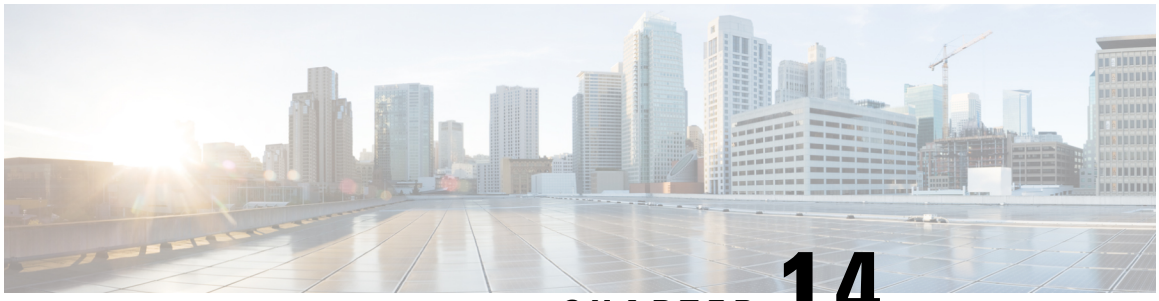
Step 3 Click **Go**. The policies for that interface are displayed.

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.

Step 6 Click **Apply**. The QoS policy binding is defined, and the Running Configuration file is updated.



CHAPTER 14

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 181
- SNMP Views, on page 182
- SNMP Groups, on page 183
- SNMP Users, on page 184
- SNMP Communities, on page 185
- Notification Recipients SNMPv1,2, on page 186
- Notification Recipients SNMPv3, on page 187

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).

To configure the SNMP engine ID, complete the following steps:

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

- 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.
- Server IP Address/Name—Enter the IP address or domain name of the SNMP 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 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 183.

To configure the SNMP views, complete the following steps:

Step 1 Click **SNMP** > **Views**.

The following fields are displayed for each view:

- View Name —The name of SNMP 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.

- All—Default SNMP view for read and read/write 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 182.

To create an SNMP group, complete the following steps:

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.

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 181 .
- An SNMPv3 group must be available. An SNMPv3 group is defined in the SNMP Groups, on page 183 .

To display SNMP users and define new ones:

Step 1 Click **SNMP** > **Users**.

This page displays existing users. The fields in this page are described in the Add page.

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.
- 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—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 184).
- Advanced Mode—The access rights of a community are defined by a group (defined in the SNMP Groups, on page 183). 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:

Step 1 Click **SNMP** > **Communities**.

Step 2 Click **Add**to define and configure new SNMP community.

Step 3 Configure the following fields:

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.

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.

To define a recipient in SNMPv1,2:

Step 1 Click **SNMP** > **Notification Recipients SNMPv1,2**.

This page displays recipients for SNMPv1,2.

Step 2 Click **Add.**

Step 3 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.
- 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 185.
- 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.

Step 4 Click **Apply**. The SNMP Notification Recipient settings are written to the Running Configuration file.

Notification Recipients SNMPv3

To define a recipient in SNMPv3:

Step 1 Click **SNMP** > **Notification Recipients SNMPv3**.

Step 2 Click **Add.**

Step 3 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.
- 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.

Step 4 Click **Apply**. The SNMP Notification Recipient settings are written to the Running Configuration file.