ADMINISTRATION GUIDE

Cisco 220 Series Smart Switches Administration Guide Release 1.1.0.x

March 2020

Contents

1

Getting Started

This chapter provides an introduction to the web-based interface of the Cisco 220 switch and includes the following topics:

- **Getting Started with the Web-based Interface**
- **Quick Start Switch Configuration**
- **Interface Naming Conventions**
- **Window Navigation**

Getting Started with the Web-based Interface

The Cisco 220 switch can be accessed and managed by two methods; over your IP network by using the web-based interface, or by using the command-line interface through the console interface. Using the console interface requires advanced user skills. See the *Cisco 220 Series Smart Switches Command Line Interface Reference Guide* for more information about using the console interface.

This section includes the following topics:

- **Before You Begin**
- **Logging In to the Web-based Interface**
- **HTTP/HTTPS**
- **Changing the Administrative Password**
- **Logging Out**

Before You Begin

Before you begin to use the web-based interface, make sure that you have a computer with Internet Explorer 8.0 (or higher), Firefox 20.0 (or higher), Chrome 23.0 (or higher), or Safari 5.7 (or higher).

These are the default settings used when configuring your switch for the first time:

Parameter	Default Value
Username	**cisco**
Password	**cisco**
Switch IP	**192.168.1.254**

Logging In to the Web-based Interface

To access the switch with the web-based interface, you must know the IP address that the switch is using. The default configuration of the switch is to use its factory default IP address of **192.168.1.254** until it has obtained an IP address from a DHCP server.

NOTE 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 the switch.

You can connect to the same IP subnet as the switch by connecting them directly with an Ethernet cable, or by connecting to the same LAN where the switch is located through other switches. You can also connect your computer to the switch from another IP subnet through one or more IP routers.

STEP 3 Locate the IP address of the switch.

a. The switch can be accessed and managed by Cisco network tools and services including the Cisco FindIT Network Discovery Utility which enables you to automatically discover all supported Cisco devices in the same local network segment as your computer. You can get a snapshot view of each

device or launch the product configuration utility to view and configure the settings. For more information about FindIT, see www.cisco.com/go/findit.

b. Locate the IP address assigned by your DHCP server by accessing your router or DHCP server; see your DHCP server instructions for information. Make sure that your DHCP server is running and can be reached.

STEP 4 Set up the IP configuration on your computer.

- If the switch is using the default static IP address of **192.168.1.254**, you must choose an IP address in the range of 192.168.1.2 to 192.168.1.253 that is not already in use.
- 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 5 Open a web browser window. If you are prompted to install an Active-X plug-in when connecting to the switch, follow the prompts to accept the plug-in.

STEP 6 Enter the IP address of the switch that you are configuring in the address bar on the browser, and then press **Enter**. For example, **http://192.168.1.254**.

STEP 7 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** and the default password is **cisco**. Both username and password are case sensitive.

STEP 8 Click **Log In**.

The first time that you log in with the default username and password, you are required to enter a new password. The Change Password page opens.

HTTP/HTTPS

You can either open an HTTP session (not secured) by clicking **Log In**, or you can open an HTTPS (secured) session by clicking **Secure Browsing (HTTPS)**. You are asked to approve the logon with a default RSA key, and an HTTPS session is opened.

NOTE You do not need to input the username or password before clicking **Secure Browsing (HTTPS)**.

Changing the Administrative Password

For security purposes, you are required to change the administrative password at your first login or when the current administrative password expires.

Password complexity is enabled by default. The minimum password complexity requirements are shown on the page. The new password must comply with the default complexity rules, or it can be disabled temporarily by selecting **Disable Password Strength Enforcement**. See the **Configuring Password Complexity Rules** section for more details about password complexity.

To change the password:

STEP 1 Enter the following fields to set a new administrative password:

- **Old Password**—Enter the current password (default is **cisco**).
- **Password**—Enter a new password.
- **Confirm Password**—Enter the new password again for confirmation.
- **Password Strength Meter**—Displays the strength of the new password.
- **Disable Password Strength Enforcement**—The password strength enforcement enabled by default requires the password to conform to the following default settings:
  - Is different from the current username.
  - Has a minimum length of eight characters.
  - Contains characters from at least three character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard).

  NOTE If you do not want to change the password, check **Disable Password Strength Enforcement** and click **Apply**.

STEP 2 Click **Apply**.

The Getting Started page opens. You are now ready to configure the switch.

STEP 3 Check **Do not show this page on startup** to prevent the Getting Started page from being displayed each time that you log on to the switch. If you select this option, the System Summary page is opened instead of the Getting Started page.

Logging Out

By default, the application logs out after ten minutes of inactivity. You can change this default value as described in the **Defining Idle Session Timeout** section.

CAUTION Unless the Running Configuration is copied to the Startup Configuration, all changes made since the last time the file was saved are lost if the switch is rebooted. Save the Running Configuration to the Startup Configuration before logging off to preserve any changes that you made during this session.

A red **X** icon displayed to the left of the **Save** application link indicates that Running Configuration changes that have been made have not yet been saved to the Startup Configuration file. The flashing red **X** can be displayed by clicking the **Disable Save Icon Blinking** button on the Copy/Save Configuration page.

When the switch auto-discovers a device, such as an IP phone, it configures the port appropriately for the device. These configuration commands are written to the Running Configuration file. This operation causes the **Save** icon to begin blinking when the user logs on even though the user did not make any configuration changes.

When you click **Save**, the Copy/Save Configuration page is displayed. Save the Running Configuration file by copying it to the Startup Configuration file. After this save, the red **X** icon and the **Save** application link are no longer displayed.

To log out, click **Logout** at the top right corner of any page. The system logs out of the switch.

When a timeout occurs or you intentionally log out of the switch, a message is displayed and the login page opens with a message indicating the logged-out state. After you log in, the application returns to the initial page.

The initial page displayed depends on the "**Do not show this page on startup**" option on the Getting Started page. If you did not select this option, the initial page is the Getting Started page. If you did select this option, the initial page is the System Summary page.

Quick Start Switch Configuration

To simplify switch configuration through quick navigation, the Getting Started page provides links to the most commonly used pages.

Category	Link Name (on the Page)	Linked Page
Initial Setup	Change Management Applications and Services	Security > TCP/UDP Services page
	Change Device IP Address	Administration > Management Interface > IPv4 Interface page
	Create VLAN	VLAN Management > Create VLAN page
	Configure Port Settings	Port Management > Port Setting page
Device Status	System Summary	Status and Statistics > System Summary page
	Port Statistics	Status and Statistics > Interface page
	RMON Statistics	Status and Statistics > RMON > Statistics page
	View Log	Status and Statistics > View Log > RAM Memory page

Category	Link Name (on the Page)	Linked Page
Quick Access	Change Device Password	Administration > User Accounts page
	Upgrade Device Software	Administration > File Management > Upgrade/Backup Firmware/ Language page
	Backup Device Configuration	Administration > File Management > Download/Backup Configuration/Log page
	Create MAC-Based ACL	Access Control > MAC-Based ACL page
	Create IP-Based ACL	Access Control > IPv4-Based ACL page
	Configure QoS	Quality of Service > General > QoS Properties page
	Configure Port Mirroring	Administration > Diagnostics > Port and VLAN Mirroring page

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 Cisco Support Community page.

Interface Naming Conventions

Within the web-based interface, interfaces are denoted by concatenating the following elements:

- **Type of interface**—The following types of interfaces are found on the various types of devices:
  - **Fast Ethernet (10/100 bits)**—These are displayed as **FE**.
  - **Gigabit Ethernet (10/100/1000 bits)**—These are displayed as **GE**.
  - **LAG (Port Channel)**—These are displayed as **LAG**.
  - **VLAN**—These are displayed as **VLAN**.

- **Tunnel** —These are displayed as **Tunnel**.

- **Interface Number**—Port, LAG, tunnel, or VLAN ID.

Window Navigation

This section describes the features of the web-based interface.

Application Header

The Application Header appears on every page. It provides the following application links:

Application Link Name	Description
Username	Displays the name of the user logged on to the switch. The default username is **cisco**. (The default password is **cisco**)
Language Menu	This menu provides the following options: ▪ **Select a language:** Select one of the languages that appear in the menu. This language will be the web-based interface language. ▪ **Download Language:** Add a new language to the switch. To upgrade a language file, use the Upgrade/Backup Firmware/Language page. ▪ **Delete Language:** Deletes the second language on the switch. The first language (English) cannot be deleted.
Logout	Click to log out of the web-based interface.
About	Click to display the switch name and device version number.
Help	Click to display the online help.

Application Link Name	Description
Alert	The SYSLOG Alert Status icon appears when a SYSLOG message, above the *critical* severity level, is logged. Click the icon to open the RAM Memory page. After you access this page, the SYSLOG Alert Status icon is no longer displayed. To display the page when there is not an active SYSLOG message, click **Status and Statistics** > **View Log** > **RAM Memory**.
Save	A flashing red **X** icon displayed to the left of the **Save** application link indicates that Running Configuration changes have been made have not yet been saved to the Startup Configuration file. The flashing of the red **X** can be disabled on the Copy/Save Configuration page. Click **Save** to display the Copy/Save Configuration page. Save the Running Configuration file by copying it to the Startup Configuration file type on the switch. After this save, the red **X** icon and the Save application link are no longer displayed. When the switch is rebooted, it copies the Startup Configuration to the Running Configuration and sets the switch parameters according to the data in the Running Configuration.

Management Buttons

The following table describes the commonly-used buttons that appear on various pages in the system.

Button Name	Description
Add	Click to display the related Add page and add an entry to a table. Enter the information and click **Apply** to save it to the Running Configuration. Click **Close** to return to the main page. Click **Save** to display the Copy/Save Configuration page and save the Running Configuration to the Startup Configuration file type on the switch.

Button Name	Description
Apply	Click to apply the changes to the Running Configuration on the switch. If the switch is rebooted, the Running Configuration is lost, unless it is saved to the Startup Configuration file type or another file type. Click **Save** to display the Copy/Save Configuration page and save the Running Configuration to the Startup Configuration file type on the switch.
Cancel	Click to reset the changes made on the page.
Clear All Interfaces Counters	Click to clear the statistics counters for all interfaces.
Clear Interface Counters	Click to clear the statistics counters for the selected interface.
Clear Logs	Clears log files.
Clear Table	Clears table entries.
Close	Returns to the main page. If any changes were not applied to the Running Configuration, a message appears.
Copper Test	Click **Copper Test** to perform the related test.
Copy Settings	A table typically contains one or more entries containing configuration settings. Instead of modifying each entry individually, it is possible to modify one entry and then copy the selected entry to multiple entries, as described here: 1. Select the entry to be copied and click **Copy Settings**. 2. Enter the destination entry numbers in the **to** field. 3. Click **Apply** to save the changes and click **Close** to return to the main page.
Delete	After selecting an entry in the table, click **Delete** to remove.
Details	Click to display the details associated with the entry selected.

Button Name	Description
Edit	Select the entry and click **Edit**. The Edit page appears, and the entry can be modified. 1. Click **Apply** to save the changes to the Running Configuration. 2. Click **Close** to return to the main page.
Go	Enter the query filtering criteria and click **Go**. The results are displayed on the page.
Refresh	Click to manually refresh the data on the page.
View All Interfaces Statistics	Click to see the statistics counters for all interfaces on a single page.
View Interface Statistics	Click to see the statistics counters for the selected interface on a single page.

2

Status and Statistics

This chapter describes how to view switch statistics, and includes the following topics:

- Viewing Ethernet Interface
- Viewing Etherlike Statistics
- Viewing TCAM Utilization
- Viewing Fan Status and Temperature
- Managing RMON

Viewing Ethernet Interface

The Interface page displays traffic statistics per interface. The refresh rate of the information can be selected. This page is useful for analyzing the amount of traffic that is both sent and received and its dispersion (Unicast, Multicast, and Broadcast).

To view Ethernet statistics and/or set the refresh rate:

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

STEP 2 Enter the following information:

- **Interface**—Select the port or LAG for which the Ethernet statistics are displayed.
- **Refresh Rate**—Select the time period that passes before the Ethernet statistics are refreshed. The available options are:
  - *No Refresh*—Statistics are not refreshed.
  - *15 sec*—Statistics are refreshed every 15 seconds.
  - *30 sec*—Statistics are refreshed every 30 seconds.

- *60 sec*—Statistics are refreshed every 60 seconds.

The **Receive Statistics** area displays the following fields about incoming packets:

- **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.

The **Transmit Statistics** area displays the following fields about outgoing packets:

- **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.

STEP 3 Click **Clear Interface Counters** to clear the statistics counters for the selected interface.

STEP 4 Click **Refresh** to manually refresh the statistics counters for the selected interface.

STEP 5 Click **View All Interfaces Statistics** to see the statistics counters for all interfaces on a single page. The Interface Statistics Table displays the statistics counters for all interfaces. From this page you can perform the following actions:

- 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.

Viewing Etherlike Statistics

The Etherlike page displays statistics per interface 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), which might disrupt traffic.

To view Etherlike statistics and/or set the refresh rate:

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

STEP 2 Enter the following information:

- **Interface**—Select the port or LAG for which the Etherlike statistics are displayed.
- **Refresh Rate**—Select the time period that passes before the Etherlike statistics are refreshed.

The following fields are displayed for the selected interface:

- **Frame Check Sequence (FCS) Errors**—Number of received frames that failed the Cyclic Redundancy Checks (CRC).
- **Single Collision Frames**—Number of frames involved in a single collision, but were successfully transmitted.
- **Late Collisions**—Number of collisions that have been detected after the first 512 bits of data.
- **Excessive Collisions**—Number of transmissions due to excessive collisions.
- **Oversize Packets**—Number of packets greater than 1518 octets received.
- **Internal MAC Receive Errors**—Number of frames rejected because of receiver errors.
- **Pause Frames Received**—Number of received flow control pause frames.
- **Pause Frames Transmitted**—Number of flow control pause frames transmitted from the selected interface.

STEP 3 Click **Clear Interface Counters** to clear the statistics counters for the selected interface.

STEP 4 Click **Refresh** to manually refresh the statistics counters for the selected interface.

STEP 5 Click **View All Interfaces Statistics** to see the statistics counters for all interfaces on a single page. The **Etherlike Statistics Table** displays the statistics counters for all interfaces. From this page you can perform the following actions:

- 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.

Viewing TCAM Utilization

The switch architecture uses a Ternary Content Addressable Memory (TCAM) to support packet actions in wire speed. TCAM holds the rules produced by applications (such as ACL and QoS) and the system-created rules.

Only system application allocates rules upon its initiation.

To view TCAM utilization, click **Status and Statistics** > **TCAM Utilization**.

The following fields are displayed:

- **Maximum TCAM Entries**—Maximum TCAM entries available.
- **In Use**—Number of TCAM entries that are currently using.

Viewing Fan Status and Temperature

The Fan and Thermal Status page displays the fan and temperature status of the switches with PoE capabilities.

The following table lists the number of fan channels and temperature channels applicable on different PoE switch models:

Model	Number of Fan Channels	Number of Temperature Channels
SF220-24P	2	2
SF220-48P	4	2
SG220-26P	2	2
SG220-28MP	3	2
SG220-50P	4	2

To view the fan and temperature status, click **Status and Statistics** > **Fan and Thermal Status**.

The following fields are displayed:

- **FAN *x* Status**—Displays the operation status of the switch fans.
  - *Operational Status*—Displays OK if the fan operates normally, or displays Fault if the fan does not operate normally.
  - *Speed Value*—Displays the fan speed in revolutions per minute (RPM).
- **Thermal *x* Status**—Displays the status of the switch thermals.
  - *Operational Status*—Displays OK when the thermal operates normally, or displays Fault when the thermal does not operate normally.
  - *Temperature Value*—Displays the current temperature in Celsius.

- *Temperature Status*—Displays the current temperature status. The possible values are:

  Green—Indicates that the current temperature is lower than the yellow threshold.

  Yellow—Indicates that the current temperature is greater than the yellow threshold, but lower than the red threshold.

  Red—Indicates that the current temperature is greater than the red threshold.

- *Yellow Threshold*—Displays the yellow threshold value of the temperature thermal.

- *Red Threshold*—Displays the red threshold value of the temperature thermal.

The following table lists the yellow and red threshold values for two thermals applicable on different PoE switch models:

Model	Yellow Threshold of Thermal 1	Red Threshold of Thermal 1	Yellow Threshold of Thermal 2	Red Threshold of Thermal 2
SF220-24P	158°F (70°C)	167°F (75°C)	171°F (77°C)	180°F (82°C)
SF220-26P	203°F (95°C)	210°F (99°C)	178°F (81°C)	185°F (85°C)
SF220-28MP	167°F (75°C)	176°F (80°C)	152°F (67°C)	162°F (72°C)
SF220-48P	147°F (64°C)	156°F (69°C)	156°F (69°C)	165°F (74°C)
SF220-50P	158°F (70°C)	167°F (75°C)	167°F (75°C)	176°F (80°C)

Managing RMON

Remote Networking Monitoring (RMON) is an SNMP specification that enables an SNMP agent in the switch 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 right thresholds set relative to your network's base line.

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

With this feature, you can perform the following actions:

- View the current statistics (since the counter values were 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 Table.
- 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).

NOTE For RMON configuration to be effective, make sure that the SNMP service is enabled on the switch.

This section includes the following topics:

- **Viewing RMON Statistics**
- **Configuring and Viewing RMON Histories**
- **Configuring and Viewing RMON Events**
- **Configuring RMON Alarms**

Viewing RMON Statistics

The Statistics page displays detailed information regarding packet sizes and some information regarding physical layer errors. The information shown is 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:

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

STEP 2 Enter the following information:

- **Interface**—Select the port or LAG for which RMON statistics are displayed.
- **Refresh Rate**—Select the time period that passes before RMON statistics are refreshed.

The following fields are displayed for the selected interface:

- **RMON Received Bytes (Octets)**—Number of octets received, including bad packets and FCS octets, but excluding framing bits.
- **RMON Drop Events**—Number of packets that were dropped.
- **RMON Received Packets** —Number of packets received, including bad packets, Multicast packets, and Broadcast packets.
- **RMON Broadcast Packets Received**—Number of good Broadcast packets received. This number does not include Multicast packets.
- **RMON Multicast Packets Received**—Number of good Multicast packets received.
- **RMON CRC & Align Errors**—Number of CRC and Align errors that have occurred.
- **RMON Undersize Packets**—Number of undersized packets (less than 64 octets) received.

- **RMON Oversize Packets**—Number of oversized packets (over 1518 octets) received.
- **RMON Fragments**—Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.
- **RMON Jabbers**—Number of received packets that were 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:
  - Packet data length is greater than MRU.
  - Packet has an invalid CRC.
  - RX error event has not been detected.
- **RMON Collisions**—Number of 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**—Number of frames, containing 64 bytes that were received.
- **Frames of 65 to 127 Bytes**—Number of frames, containing 65 to 127 bytes that were received.
- **Frames of 128 to 255 Bytes**—Number of frames, containing 128 to 255 bytes that were received.
- **Frames of 256 to 511 Bytes**—Number of frames, containing 256 to 511 bytes that were received.
- **Frames of 512 to 1023 Bytes**—Number of frames, containing 512 to 1023 bytes that were received.
- **Frames Greater than 1024 Bytes**—Number of frames, containing 1024 to 2000 bytes, and Jumbo Frames, that were received.

STEP 3 Click **Clear Interface Counters** to clear RMON statistics counters for the selected interface.

STEP 4 Click **Refresh** to manually refresh RMON statistics counters for the selected interface.

STEP 5 Click **View All Interfaces Statistics** to view RMON statistics counters for all interfaces on a single page. The RMON Statistics Table displays the RMON

statistics counters for all interfaces. From this page you can perform the following actions:

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

Configuring and Viewing RMON Histories

RMON can be used to monitor statistics per interface. Use the History Control Table page to define the sampling frequency, amount of samples to store, and the interface from where to gather the data. After the data is sampled and stored, it appears on the History Table page that can be viewed by clicking **History Table**.

Configuring RMON History Control Samples

To define RMON control sample:

STEP 1 Click **Status and Statistics** > **RMON** > **History**.

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

STEP 2 Click **Add** to add a history control sample.

STEP 3 Enter the following information:

- **New History Entry**—Displays the number of the history entry.
- **Source Interface**—Select the port or LAG from where the history samples are to be taken.
- **Max No. of Samples to Keep**—Enter the number of samples to store.

- **Interval**—Enter the time in seconds that samples were collected from the interface.
- **Owner**—Enter the RMON station or user that requested the RMON information.

STEP 4 Click **Apply**. The RMON history control sample is added, and the Running Configuration is updated.

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

Viewing RMON History Statistics

The History Table page displays interface-specific statistical network samplings. The samples are configured in the History Control Table described in the previous section.

To view RMON history statistics:

STEP 1 Click **Status and Statistics** > **RMON** > **History**.

STEP 2 Click **History Table**.

STEP 3 Select the entry number to display the samples associated with that history entry, and click **Go**.

The following fields are displayed for the selected history sample:

- **History Entry No.**—Number of the history entry.
- **Owner**—History entry owner.
- **Sample No.**—Statistics were taken from this sample.
- **Drop Events**—Number of dropped packets due to lack of network resources during the sampling interval. This field may not represent the exact number of dropped packets, but rather the number of times that dropped packets were detected.
- **Bytes Received**—Number of octets received including bad packets and FCS octets, but excluding framing bits.
- **Packets Received**—Number of packets received, including bad packets, Multicast, and Broadcast packets.
- **Broadcast Packets**—Number of good Broadcast packets received. This number does not include Multicast packets.

- **Multicast Packets**—Number of good Multicast packets received.
- **CRC & Align Errors**—Number of CRC and align errors that have occurred.
- **Undersize Packets**—Number of undersized packets (less than 64 octets) received.
- **Oversize Packets**—Number of oversized packets (over 1518 octets) received.
- **Fragments**—Number of fragments (packets with less than 64 octets) received, excluding framing bits, but including Frame Check Sequence (FCS) octets.
- **Jabbers**—Number of received packets that were longer than 1632 octets. This number excludes frame bits, but includes FCS octets that had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number.
- **Collisions**—Number of collisions received.
- **Utilization**—Percentage of current interface traffic compared to the maximum traffic that the interface can handle.

STEP 4 Click **History Control Table** to return to the History Control Table page.

Configuring and Viewing RMON Events

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

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

Configuring RMON Events

Use the Events page to configure events that are actions performed when an alarm is generated (alarms are defined on the Alarms page). An event can be any combination of logs and traps. If the action includes logging of the events, they are displayed on the Event Log Table page.

To configure RMON events:

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

STEP 2 Click **Add** to add an RMON event.

STEP 3 Enter the following information:

- **Event Entry**—Displays the number for the event entry.
- **Community**— Enter the SNMP community string to be included when traps are sent.
- **Description**—Enter a name for the event. This name is used to attach an alarm to an event.
- **Notification Type**—Select the type of action that results from this event. The available options are:
  - *None*—No action occurs when the alarm goes off.
  - *Log (Event Log Table)*—Add a log entry to the Event Log Table when the alarm goes off.
  - *Trap (SNMP Manager)*—Send a trap when 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 added, and the Running Configuration is updated.

STEP 5 Click **Event Log Table** to display the log of alarms that have occurred and that have been logged.

Viewing RMON Event Logs

The Event Log Table page displays the log of events (actions) that occurred. An event can be logged when the type of the event is *Log* or *Log and Trap*. The action in the event is performed when the event is bound to an alarm (see **Configuring RMON Alarms**) and the conditions of the alarm have occurred.

To view RMON event logs:

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

STEP 2 Click **Event Log Table**.

The following fields are displayed:

- **Event Entry No.**—Number of the event's log entry.
- **Log No.**—Log number (within the event).
- **Log Time**—Time that the log entry was entered.
- **Description**—Description of event that triggered the alarm.

STEP 3 Click **Event Table** to return to the Events page.

Configuring RMON Alarms

RMON alarms provide a mechanism for setting thresholds and sampling intervals to generate exception events on any counter 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.

Use the Alarms page to configure alarms and to bind them with events. Alarm counters can be monitored by either absolute values or changes (delta) in the counter values.

To define RMON alarms:

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

STEP 2 Click **Add** to add an RMON alarm.

STEP 3 Enter the following information:

- **Alarm Entry**—Displays the number of the alarm entry.
- **Interface**—Select a port or LAG.
- **Counter Name**—Select the MIB variable that indicates the type of occurrence measured.
- **Sample Type**—Select the sampling method to generate an alarm. The possible options are:
  - *Absolute*—If the threshold is passed, 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 is passed, an alarm is generated.
- **Rising Threshold**—Enter the rising counter value that triggers the rising threshold alarm.
- **Rising Event**—Select an event, from those that you defined on the Events page, to be performed when a rising event is triggered.
- **Falling Threshold**—Enter the falling counter value that triggers the falling threshold alarm.
- **Falling Event**—Select an event, from those that you defined on the Events page, 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 counter value triggers the rising threshold alarm.
  - *Falling Alarm*—A falling counter value triggers the falling threshold alarm.
  - *Rising and Falling Alarm*—Both a rising and falling counter 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 added, and the Running Configuration is updated.

3

Administration: System Logs

This chapter describes the System Log feature, which enables the switch to keep several independent logs. Each log is a set of messages recording system events.

The switch generates the following local logs:

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

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

This chapter covers the following topics:

- **Configuring System Log Settings**
- **Configuring Remote Logging Settings**
- **Viewing Memory Logs**

Configuring System Log Settings

You can enable or disable logging on the switch and select the events to be logged by severity level. The event severity levels are listed from the highest severity to the lowest severity:

- **Emergency**—System is not usable.
- **Alert**—Immediate 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**—Provides detailed information about an event.

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

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

To configure global log parameters:

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

STEP 2 Enter the following information:

- **Logging**—Check **Enable** to enable logging on the switch, or uncheck to disable logging on the switch.
- **RAM Memory Logging**—Check **Enable** to enable RAM memory logging and check the severity levels of the messages to be logged to RAM.
- **Flash Memory Logging**—Check **Enable** to enable flash memory logging and check the severity levels of the messages to be logged to flash memory.

STEP 3 Click **Apply**. The global log settings are defined, and the Running Configuration is updated.

Configuring Remote Logging Settings

Use the Remote Log Servers page to define the remote SYSLOG servers where log messages are sent (using the SYSLOG protocol). For each server, you can configure the severity of the messages that it receives.

To configure a remote SYSLOG server:

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

STEP 2 Click **Add** to add a remote SYSLOG server.

STEP 3 Enter the following information:

- **Server Definition**—Select whether to identify the remote log server by IP address or name.
- **IP Version**—Select either **Version 4** or **Version 6** if the remote log server is identified by IP address.
- **Log Server IP Address/Name**—Enter the IP address or hostname of the remote log server.
- **UDP Port**—Enter the UDP port to which the log messages are sent.
- **Facility**—Select a facility from which system logs are sent to the remote server. Only one facility can be assigned to a server.
- **Minimum Severity**—Select the minimum level of system log messages to be sent to the server.

STEP 4 Click **Apply**. The remote SYSLOG server is added, and the Running Configuration is updated.

Viewing Memory Logs

The switch can write to the following logs:

- Log in RAM (cleared during reboot). See **Viewing RAM Memory Logs** for more information.
- Log in flash memory (cleared only upon user command). See **Viewing Flash Memory Logs** for more information.

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

Viewing RAM Memory Logs

The RAM Memory page displays all messages that are saved in RAM (cache) in inverse-chronological order. Entries are stored in the RAM log according to the configuration on the Log Settings page.

To view RAM logs:

STEP 1 Click **Status and Statistics** > **View Log** > **RAM Memory**.

The following fields are displayed:

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

STEP 2 Click **Clear Logs** to clear the log messages.

STEP 3 By default, the SYSLOG Alert Status icon appears and blinks when a SYSLOG message above the *critical* severity level is logged. To disable this alert icon blinking, click **Disable Alert Icon Blinking**. The SYSLOG Alert Status icon is no longer displayed.

Viewing Flash Memory Logs

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

To view flash logs:

STEP 1 Click **Status and Statistics** > **View Log** > **Flash Memory**.

The following fields are displayed:

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

STEP 2 Click **Clear Logs** to clear the log messages.

4

Administration: File Management

This chapter describes how system files are managed, such as upgrading system firmware, rebooting the switch, restoring the switch to factory defaults, managing the configuration files and log files, and so on.

It includes the following topics:

- **Files and File Types**
- **File Actions**
- **Upgrade/Backup Firmware/Language**
- **Active Image**
- **Download/Backup Configuration or Logs**
- **Configuration File Properties**
- **Copy/Save Configuration Files**
- **DHCP Auto Configuration**

Files and File Types

System files are files that contain configuration information or firmware images.

Various actions can be performed with these files:

- Selecting the firmware file from which the switch boots.
- Copying various types of configuration files internally on the switch.
- Copying files to or from an external device, such as an external server.

The possible methods of file transfer are:

- Internal copy.

- HTTP/HTTPS that uses the facility that the browser provides.
- TFTP client, requiring a TFTP server.

Configuration files on the switch are defined by their type, and contain the settings and parameter values for the switch. When a configuration is referenced on the switch, it is referenced by its configuration file type (such as Startup Configuration or Running Configuration), instead of a file name that can be modified by the user. Content can be copied from one file type to another, but the names of the file types cannot be changed by the user. Other files on the switch include firmware and log files, and are referred to as operational files.

Configuration files are text files that can be edited by a user in a text editor, such as Notepad after they are copied to an external device, such as a PC.

The following types of configuration and operational files are found on the switch:

- **Running Configuration**—Contains parameters that are currently used by the switch to operate. It is the only file type that is modified when you change the parameter values on the switch.

  If the switch is rebooted, the Running Configuration is lost. When the switch is rebooted, this file type is copied from the Startup Configuration stored in flash to the Running Configuration stored in RAM.

  To preserve any changes that you made to the switch, you must save the Running Configuration to the Startup Configuration, or another file type if you do not want the switch to reboot with this configuration. If you have saved the Running Configuration to the Startup Configuration, when the switch is rebooted, it recreates a Running Configuration that includes the changes made since the last time that the Running Configuration was saved to the Startup Configuration.

- **Startup Configuration**—The parameter values that were saved by you by copying another configuration (usually the Running Configuration) to the Startup Configuration.

  The Startup Configuration is retained in flash and is preserved when the switch is rebooted. At this time, the Startup Configuration is copied to RAM and identified as the Running Configuration.

- **Backup Configuration**—A manual copy of the parameter definitions for protection against system shutdown or for the maintenance of a specific operating state. You can copy the Mirror Configuration, Startup Configuration, or Running Configuration to the Backup Configuration. The Backup Configuration exists in flash and is preserved if the switch is rebooted.

- **Mirror Configuration**—A copy of the Startup Configuration, created by the switch when the following conditions exist:
  - The switch 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.

  If the switch is rebooted, the Mirror Configuration is reset to the factory default parameters. In all other aspects, the Mirror Configuration functions the same as a Backup Configuration, providing a copy of the parameter values that is preserved if the switch is rebooted.
- **Firmware**—The program that controls the operations and functionality of the switch. More commonly referred to as the image.
- **Language File**—The dictionary that enables the web-based interface to be displayed in the selected language.
- **Flash Logs**—SYSLOG messages stored in flash memory.

File Actions

The following actions can be performed to manage firmware, configuration files, and logs:

- Upgrade the firmware image, replace a second language file, or back up the firmware as described in **Upgrade/Backup Firmware/Language** section.
- View the firmware image currently in use or select the image to be used in the next reboot as described in the **Active Image** section.
- Save configuration files on the switch to a location on another device as described in the **Download/Backup Configuration or Logs** section.
- Clear the Startup Configuration or Backup Configuration file types as described in the **Configuration File Properties** section.

- Copy one configuration file type to another configuration file type as described in the **Copy/Save Configuration Files** section.
- Automatically download a configuration file from a DHCP server to the switch as described in the **DHCP Auto Configuration** section.

CAUTION Unless the Running Configuration is manually copied to the Startup Configuration, Backup Configuration, or an external file, all changes made since the last time the file was saved are lost when the switch is rebooted. We recommend that you save the Running Configuration to the Startup Configuration before logging off to preserve any changes you made during this session.

A red **X** icon, displayed to the left of the **Save** application link, indicates that configuration changes have been made and have not yet been saved to the Startup Configuration file.

When you click **Save**, the Copy/Save Configuration page is displayed. Save the Running Configuration file by copying it to the Startup Configuration file. After this save, the red **X** icon and the Save link is hidden.

Upgrade/Backup Firmware/Language

Use the Upgrade/Backup Firmware/Language page to upgrade or backup the firmware image, and import a second language file.

The following methods for transferring files are supported:

- HTTP/HTTPS that uses the facilities provided by the browser.
- TFTP that requires a TFTP server.

Upgrading/Saving the Firmware Image

There are two firmware images, Image1 and Image2, stored on the switch. One of the images is identified as the active image and other image is identified as the inactive image.

When you upgrade the firmware, the new image always replaces the image identified as the inactive image. Even after uploading new firmware on the switch, the switch continues to boot by using the active image (the old version) until you change the status of the new image to be the active image by using the procedure described in the **Active Image** section, and boot the switch by using the process described in the **Rebooting the Switch** section.

You can also save a copy of the active image on the switch to a destination location such as a TFTP server.

To upgrade or backup the firmware image:

STEP 1 Click **Administration** > **File Management** > **Upgrade/Backup Firmware/Language**.

STEP 2 To replace the firmware image on the switch with a new version located on a TFTP server, enter the following information:

- **Transfer Method**—Select **via TFTP** as the transfer method.
- **Save Action**—Select **Upgrade** as the action.
- **File Type**—Select **Firmware Image** as the file type.
- **TFTP Server Definition**—Select whether to specify the TFTP server by IP address or domain name.
- **IP Version**—Select either **Version 4** or **Version 6** if the TFTP server is identified by IP address.
- **TFTP Server IP Address/Name**—Enter the IP address or domain name of the TFTP server.
- **Source File Name**—Enter the name of the firmware image located on the TFTP server.

STEP 3 Click **Apply**.

STEP 4 To replace the firmware image on the switch with a new version located on another device such as your local PC, enter the following information:

- **Transfer Method**—Select **via HTTP/HTTPS** as the transfer method.

- **Save Action**—Select **Upgrade** as the action.
- **File Type**—Select **Firmware Image** as the file type.
- **File Name**—Click **Browse** to select a firmware image located on another device such as your local PC.

STEP 5 Click **Apply**.

STEP 6 To save a copy of the active image on the switch to a TFTP server, enter the following information:

- **Transfer Method**—Select **via TFTP** as the transfer method.
- **Save Action**—Select **Backup** as the action.
- **File Type**—Select **Firmware Image** as the file type.
- **TFTP Server Definition**—Select whether to specify the TFTP server by IP address or domain name.
- **IP Version**—Select either **Version 4** or **Version 6** if the TFTP server is identified by IP address.
- **TFTP Server IP Address/Name**—Enter the IP address or domain name of the TFTP server.
- **Destination File Name**—Enter the name of the firmware image that will be saved to the TFTP server.

STEP 7 Click **Apply**.

Upgrading the Language File

If a new language file was loaded onto the switch, the new language can be selected from the **Language** drop-down menu. (It is not necessary to reboot the switch.)

To upload a new language file:

STEP 1 Click **Administration** > **File Management** > **Upgrade/Backup Firmware/Language**.

STEP 2 To upload a language file from a TFTP server to the switch, enter the following information:

- **Transfer Method**—Select **via TFTP** as the transfer method.

- **Save Action**—Select **Upgrade** as the action.
- **File Type**—Select **Language File** as the file type.
- **TFTP Server Definition**—Select whether to specify the TFTP server by IP address or domain name.
- **IP Version**—Select either **Version 4** or **Version 6** if the TFTP server is identified by IP address.
- **TFTP Server IP Address/Name**—Enter the IP address or domain name of the TFTP server.
- **Source File Name**—Enter the name of the source language file located on the TFTP server.

STEP 3 Click **Apply**.

STEP 4 To upload a language file from another device such as your local PC to the switch, do the following:

- **Transfer Method**—Select **via HTTP/HTTPS** as the transfer method.
- **Save Action**—Select **Upgrade** as the action.
- **File Type**—Select **Language File** as the file type.
- **File Name**—Click **Browse** to select a new language file located on another device such as your local PC.

STEP 5 Click **Apply**.

Active Image

There are two firmware images, Image1 and Image2, stored on the switch. One of the images is identified as the active image and other image is identified as the inactive image. The switch boots from the image you set as the active image. You can change the image identified as the inactive image to the active image. (You need to reboot the switch.)

To select the active image:

STEP 1 Click **Administration** > **File Management** > **Active Image**.

The following fields are displayed:

- **Active Image**—Displays the image file that is currently active on the switch.
- **Active Image Version Number**—Displays the firmware version of the active image.
- **Active Image Version Number After Reboot**—Displays the firmware version of the active image after reboot.

STEP 2 Select the image from the **Active Image After Reboot** drop-down menu to identify the firmware image that is used as the active image after the switch is rebooted.

STEP 3 Click **Apply**.

STEP 4 Reboot the switch. The switch will boot with the selected active image.

Download/Backup Configuration or Logs

The Download/Backup Configuration/Log page enables:

- Backing up of configuration files or logs from the switch to an external device.
- Restoring configuration files from an external device to the switch.

When restoring a configuration file to the Running Configuration, the imported file adds any configuration commands that do not exist in the old file and overwrites any parameter values in the existing configuration commands.

When restoring a configuration file to the Startup Configuration or the Backup Configuration file, the new file replaces the previous file.

When restoring to the Startup Configuration, the switch must be rebooted for the restored Startup Configuration to be used as the Running Configuration.

Uploading Configuration File

To replace a file type with a saved configuration file:

STEP 1 Click **Administration** > **File Management** > **Download/Backup Configuration/ Log**.

STEP 2 To replace a file type on the switch with a version of that file type on a TFTP server, enter the following information:

- **Transfer Method**—Select **via TFTP** as the transfer method.
- **Save Action**—Select **Download** as the action.
- **TFTP Server Definition**—Select whether to specify the TFTP server by IP address or domain name.
- **IP Version**—Select either **Version 4** or **Version 6** if the TFTP server is identified by IP address.
- **TFTP Server IP Address/Name**—Enter the IP address or domain name of the TFTP server.
- **Source File Name**—Enter the source file name.
- **Destination File Type**—Select the configuration file type to be upgraded. The switch supports upgrading the Running Configuration, Startup Configuration, and Backup Configuration.

STEP 3 Click **Apply**. The file is upgraded on the switch (depending upon the file type).

STEP 4 To replace a file type on the switch with a version of that file type on another device such as your local PC, enter the following information:

- **Transfer Method**—Select **via HTTP/HTTPS** as the transfer method.
- **Save Action**—Select **Download** as the action.
- **File Name**—Click **Browse** to select a source file.
- **Destination File Type**—Select the configuration file type to be upgraded.

STEP 5 Click **Apply**. The file is transferred from the other device to the switch.

Saving Configuration File or Logs

To copy configuration file types or the flash log on the switch to a file on another device:

STEP 1 Click **Administration** > **File Management** > **Download/Backup Configuration/ Log**.

STEP 2 To copy a file type on the switch to a file on a TFTP server, enter the following information:

- **Transfer Method**—Select **via TFTP** as the transfer method.
- **Save Action**—Select **Backup** as the action.
- **TFTP Server Definition**—Select whether to specify the TFTP server by IP address or domain name.
- **IP Version**—Select either **Version 4** or **Version 6** if the TFTP server is identified by IP address.
- **TFTP Server IP Address/Name**—Enter the IP address or domain name of the TFTP server.
- **Source File Type**—Select the configuration file type to be stored on the TFTP server. The switch supports storing the Running Configuration, Startup Configuration, Backup Configuration, Mirror Configuration, and the flash log.
- **Destination File Name**—Enter the file name to be stored on the TFTP server.

STEP 3 Click **Apply**. The file is backed up on the TFTP server (depending upon the file type).

STEP 4 To copy a file type on the switch to a file on another device such as your local PC, enter the following information:

- **Transfer Method**—Select **via HTTP/HTTPS** as the transfer method.
- **Save Action**—Select **Backup** as the action.
- **Source File Type**—Select the configuration file type to be stored.

STEP 5 Click **Apply**.

STEP 6 Locate where to save the selected configuration file or flash log, click **Save**.

Configuration File Properties

Use the Configuration Files Properties page to see when various system configuration files are created. It also enables deleting the Startup Configuration and Backup Configuration files. You cannot delete the other configuration file types.

To clear configuration files and/or see when configuration files are created:

STEP 1 Click **Administration** > **File Management** > **Configuration Files Properties**.

The following fields are displayed:

- **Configuration File Name**—The type of file.
- **Creation Time**—The date and time that file was modified.

STEP 2 If required, select either the Startup Configuration, Backup Configuration, or both and click **Clear Files** to delete these files.

Copy/Save Configuration Files

When you click **Apply** on any window, changes that you made to the switch configuration settings are stored only in the Running Configuration. To preserve the parameters in the Running Configuration, the Running Configuration must be copied to another configuration type or saved as a file on another device.

Use the Copy/Save Configuration page to copy or save one configuration file to another for backup purposes. The bottom of the page has a button, **Disable Save Icon Blinking**. Click to toggle between disable and enable.

CAUTION Unless the Running Configuration is copied to the Startup Configuration or another configuration file, all changes made since the last time the file was copied are lost when the switch is rebooted.

The following combinations of copying internal file types are allowed:

- From the Running Configuration to the Running Configuration, Startup Configuration or Backup Configuration.
- From the Startup Configuration to the Running Configuration, Startup Configuration, or Backup Configuration.
- From the Backup Configuration to the Running Configuration, Startup Configuration, or Backup Configuration.
- From the Mirror Configuration to the Running Configuration, Startup Configuration, or Backup Configuration.

To copy one type of configuration file to another type of configuration file:

STEP 1 Click **Administration** > **File Management** > **Copy/Save Configuration**.

STEP 2 Enter the following information:

- **Source File Name**—Select the configuration file type to be copied.
- **Destination File Name**—Select the configuration file type to be overwritten by the source file.

STEP 3 Click **Apply**. The file is copied and the switch is updated.

STEP 4 The **Save Icon Blinking** field indicates whether an icon blinks when there is unsaved data. To disable or enable this feature, click **Disable Save Icon Blinking** or **Enable Save Icon Blinking**.

DHCP Auto Configuration

Auto Configuration enables passing configuration information to hosts on a TCP/IP network. Based on this protocol, the Auto Configuration feature enables the switch to download configuration files from a TFTP server.

By default, the switch is enabled as a DHCP client when the Auto Configuration feature is enabled. The switch can be configured as a DHCPv4 client in which auto configuration from a DHCPv4 server is supported and/or a DHCPv6 client in which auto configuration from a DHCPv6 server is supported.

NOTE DHCP Auto Configuration will not trigger when there is a "startup-config file in switch. This feature only works when the switch starts from the default state.

DHCPv4 Auto Configuration is triggered in the following cases:

- After rebooting the switch when an IP address is allocated or renewed dynamically (using DHCPv4).
- Upon an explicit DHCPv4 renewal request and if the switch and the server are configured to do so.

DHCPv6 Auto Configuration is triggered when the following conditions are fulfilled:

- When a DHCPv6 server sends information to the switch. This occurs in the following cases:
  - When IPv6 stateless client is enabled.
  - When DHCPv6 messages are received from the server.
  - When DHCPv6 information is refreshed by the switch.
  - After rebooting the switch when stateless DHCPv6 client is enabled.
- When the DHCPv6 server packets contain the configuration filename option.

DHCP Server Options

DHCP messages may contain the configuration server name/address and the configuration file name/path (these are optional options). These options are found in the Offer message coming from the DHCPv4 servers and in the Information Reply messages coming from DHCPv6 servers.

Backup information (configuration server name/address and configuration file name/path) can be configured on the DHCP Auto Configuration page. This information is used when the DHCPv4 or DHCPv6 message does not contain this information.

Auto Configuration Process

When the Auto Configuration process is triggered, the following sequence of events occurs:

- The DHCP server is accessed to acquire the TFTP server name/ address and configuration file name/path (DHCPv4 options: 66,150, and 67, DHCPv6 options: 59 and 60).
- If a server and configuration file options are not supplied by the DHCP server, the user-defined, backup configuration file name is used for DHCPv4 or DHCPv6.
- If the DHCP server does not send these options and the backup TFTP server address parameter is empty, then the switch sends TFTP request messages to limited Broadcast IPv4 address and continues the process of Auto Configuration with the first answering TFTP server.

Configuring DHCP Auto Configuration Parameters

To configure DHCP Auto Configuration, you need to perform the following:

- Configure the DHCPv4 and/or DHCPv6 servers to send the required options. This process is not described in this guide.
- Configure the DHCP Auto Configuration parameters as described in this section.
- Set the IP Address Type to Dynamic on the IPv4 Interface page, as described in the **IPv4 Management and Interface** section.

Use the DHCP Auto Configuration page to perform the following actions when the information is not provided in a DHCP message:

- Enable the DHCP Auto Configuration feature.

- Configure the switch to receive configuration information from a specific file on a specific server.

Note the following regarding the DHCP Auto Configuration process:

- A configuration file that is placed on the TFTP server must match the form and format requirements of the supported configuration file. The form and format of the file are checked, but the validity of the configuration parameters is not checked prior to loading it to the Startup Configuration.
- In IPv4, different IP addresses are allocated with each DHCP renewal cycle. To ensure that the device configuration functions as intended, we recommend that IP addresses be bound to MAC addresses in the DHCP server table.

NOTE DHCP Auto Configuration is applicable only when the IP address of the switch is set to dynamic.

To configure DHCP Auto Configuration:

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

STEP 2 Enter the following information:

- **Auto Configuration via DHCP**—Check **Enable** to enable the DHCP Auto Configuration feature on the switch, or uncheck to disable this feature.
- **Backup Server Definition**—Select whether to specify the TFTP server by IP address or domain name.
- **IP Version**—Select either **Version 4** or **Version 6** if the TFTP server is identified by IP address.
- **Backup TFTP Server IP Address/Name**—Enter the IP address or domain name of the backup TFTP server. If no configuration file name is specified in the DHCP message, the switch will download the backup configuration file from the backup TFTP server.
- **Backup Configuration File**—Enter the full file path and name of the configuration file on the backup TFTP server to be used if no configuration file name is specified in the DHCP message.
- **Last Auto Configuration TFTP Server IP Address**—Displays the IP address or domain name of the TFTP server that is currently using.
- **Last Auto Configuration File Name**—Displays the name of the configuration file located on the TFTP server that is currently using.

STEP 3 Click **Apply**. The DHCP Auto Configuration parameters are defined, and the Running Configuration is updated.

5

Administration: General Information

This chapter describes how to view system information and configure various options on the switch.

It includes the following topics:

- Device Models
- Viewing System Summary
- Configuring System Settings
- Configuring Console Settings
- Rebooting the Switch
- Defining Idle Session Timeout
- Ping a Host
- Using Traceroute

Device Models

All models can be fully managed through the web-based interface. The following table describes the various models, the number and type of ports on them, and their PoE and PID information:

Model Name	Ports and Expansion Ports	Ports that Support PoE	PIDs
Fast Ethernet			
SF220-24	24 FE copper ports and 2 special-purpose combo ports (GE/SFP)	N/A	SF220-24-K9-NA, SF220-24-K9-EU, SF220-24-K9-UK, SF220-24-K9-AU, SF220-24-K9-CN
SF220-24P	24 FE copper ports and 2 special-purpose combo ports (GE/SFP)	1 to 24	SF220-24P-K9-NA, SF220-24P-K9-EU, SF220-24P-K9-UK, SF220-24P-K9-AU, SF220-24P-K9-CN
SF220-48	48 FE copper ports and 2 special-purpose combo ports (GE/SFP)	N/A	SF220-48-K9-NA, SF220-48-K9-EU, SF220-48-K9-UK, SF220-48-K9-AU, SF220-48-K9-CN
SF220-48P	48 FE copper ports and 2 special-purpose combo ports (GE/SFP)	1 to 48	SF220-48P-K9-NA, SF220-48P-K9-EU, SF220-48P-K9-UK, SF220-48P-K9-AU, SF220-48P-K9-CN
Gigabit Ethernet			
SG220-26	24 GE copper ports and 2 special-purpose combo ports (GE/SFP)	N/A	SG220-26-K9-NA, SG220-26-K9-EU, SG220-26-K9-UK, SG220-26-K9-AU, SG220-26-K9-BR, SG220-26-K9-AR

Model Name	Ports and Expansion Ports	Ports that Support PoE	PIDs
SG220-26P	24 GE copper ports and 2 special-purpose combo ports (GE/SFP)	1 to 24	SF220-26P-K9-NA, SF220-26P-K9-EU, SF220-26P-K9-UK, SF220-26P-K9-AU, SF220-26P-K9-BR, SF220-26P-K9-AR
SG220-50	48 GE copper ports and 2 special-purpose combo ports (GE/SFP)	N/A	SG220-50-K9-NA, SG220-50-K9-EU, SG220-50-K9-UK, SG220-50-K9-AU, SG220-50-K9-BR, SG220-50-K9-AR
SG220-50P	48 GE copper ports and 2 special-purpose combo ports (GE/SFP)	1 to 48	SF220-50P-K9-NA, SF220-50P-K9-EU, SF220-50P-K9-UK, SF220-50P-K9-AU, SF220-50P-K9-BR, SF220-50P-K9-AR
SG220-28	24 GE copper ports and 4 SFP ports	N/A	SG220-28-K9-CN
SG220-28MP	24 GE copper ports and 4 SFP ports	1 to 24	SG220-28MP-K9-CN
SG220-52	48 GE copper ports and 4 SFP ports	N/A	SG220-52-K9-CN

NOTE There are some features applicable only for the models with specific country of destination (-CN), indicating that these features are only applicable for their China SKUs. These features are noted in this guide. You can find the PID information of your switch from the System Summary page.

Viewing System Summary

The System Summary page provides a graphic view of the switch, and displays general switch information, including system information, software information, PoE power information (if applicable), TCP/UDP services status, and other items.

To view general switch information, click **Status and Statistics** > **System Summary**. The following fields are displayed:

System Information

- **System Description**—A description of the switch.
- **System Location**—Physical location of the switch.
- **System Contact**—Name of a contact person.
- **Host Name**—Name of the switch. By default, the switch's hostname is composed of the word *Switch* concatenated with the three least significant bytes of the switch MAC address (the six furthest right hexadecimal digits).

  NOTE You can click **Edit** to go to the Administration > System Settings page to edit the location, contact, and/or hostname.
- **System Object ID**—Unique vendor identification of the network management subsystem contained in the SNMP entity.
- **System Uptime**—Time that has elapsed since the last reboot.
- **Current Time**—Current system time.
- **Base MAC Address**—MAC address of the switch.
- **Jumbo Frames**—Jumbo frame support status. This support can be enabled or disabled on the Port Management > Port Setting page.

  NOTE Jumbo frames support takes effect only after it is enabled, and after the switch is rebooted.

Software Information

- **Firmware Version (Active Image)**—Version number of the active firmware image.
- **Firmware MD5 Checksum (Active Image)**—MD5 checksum of the active firmware image.
- **Firmware Version (Non-active)**—Version number of the non-active firmware image.

- **Firmware MD5 Checksum (Non-active Image)**—MD5 checksum of the non-active firmware image.
- **Boot Version**—Version number of the switch's bootloader.
- **Locale**—Locale of the first language. (This is always en-US.)
- **Language Version**—Language package version of the first language.
- **Language MD5 Checksum**—MD5 checksum of the first language.
- **Locale**—Locale of the second language.
- **Language Version**—Language package version of the second language.
- **Language MD5 Checksum**—MD5 checksum of the second language.

TCP/UDP Services Status

- **HTTP Service**—Shows whether the HTTP service is enabled or disabled.
- **HTTPS Service**—Shows whether the HTTPS service is enabled or disabled.
- **SNMP Service**—Shows whether the SNMP service is enabled or disabled.
- **Telnet Service**—Shows whether the Telnet service is enabled or disabled.
- **SSH Service**—Shows whether the SSH service is enabled or disabled.

  NOTE You can click **Edit** to go to the Security > TCP/UDP Services page to enable or disable these services on the switch.

PoE Power Information (only applicable for the PoE models)

- **Maximum Available PoE Power (W)**—Maximum available power that can be delivered by the PoE ports.
- **Total PoE Power Consumption (W)**—Total PoE power delivered to the connected PoE devices.
- **PoE Power Mode**—Port Limit or Class Limit.

  NOTE You can click **Detail** to go to the Port Management > PoE > PoE Properties page to see more details about the PoE settings.

Other Summary Information

- **Serial Number**—Serial number.
- **PID VID**—Part number and version ID.

Configuring System Settings

To view or modify system settings:

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

STEP 2 View or modify the following system settings:

- **System Description**—Displays the description of the switch.
- **System Location**—Enter the location where the switch is physically located.
- **System Contact**—Enter the name of a contact person.
- **Host Name**—Select how to define the hostname of the switch. The available options are:
  - *Use Default*—Use the default hostname (System Name). The default hostname of the switch is *switch123456*, where 123456 indicates the last three bytes of the switch MAC address in hex format.
  - *User Defined*—Manually enter the hostname of the switch. Use only letters, digits, and hyphens. Hostnames cannot begin or end with a hyphen. No other symbols, punctuation characters, or blank spaces are permitted (as specified in RFC1033, 1034, 1035).

STEP 3 In the **Custom Login Screen Settings** area, specify the system banners that are displayed when users try to access the switch. The available banners are:

- **Login Banner**—Enter the text message that is displayed before the login prompt of username and password (generally shown on the login page). The message is maximum 2000 characters long. Click **Preview** to preview your settings.
- **Welcome Banner**—Enter the text message that is displayed when an EXEC process is created. The message is maximum 2000 characters long. Click **Preview** to preview your settings.

  NOTE The banners defined on the web-based interface can also be activated on the command-line interfaces (Console, Telnet, and SSH).

STEP 4 Click **Apply**. The system settings are modified, and the Running Configuration is updated.

Configuring Console Settings

Use the Console Settings page to configure the console port Baud rate. The default console port settings are displayed as follows:

- 9,600 bits per second
- 8 data bits
- no parity
- 1 stop bit
- no flow control

To change the console port Baud rate:

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.

Rebooting the Switch

Some configuration changes require the switch to be rebooted before they take effect. However, rebooting the switch will delete the Running Configuration, so it is critical that the Running Configuration is saved to the Startup Configuration before the switch is rebooted. Clicking **Apply** does not save the configuration to the Startup Configuration.

You can save the Running Configuration on the **Administration** > **Save/Copy Configuration** page or click **Save** at the top of the window.

To reboot the switch:

STEP 1 Click **Administration** > **Reboot**.

STEP 2 Click **Reboot** to reboot the switch. Because any unsaved information in the Running Configuration is discarded when the switch is rebooted, you must click

Save in the upper-right corner of any window to preserve current configuration across the boot process. (If the **Save** option is not displayed, the Running Configuration matches the Startup Configuration and no action is necessary.)

STEP 3 You can also check **Enable** next to the **Reboot to Factory Defaults** field and click **Reboot** to reboot the switch by using factory default configuration. This process erases the Startup Configuration file; any settings that are not saved to another file are cleared when this action is selected.

The Mirror Configuration is not deleted when restoring to factory defaults.

Defining Idle Session Timeout

Use the Idle Session Timeout page to configure the time intervals that the management sessions can remain idle before they timeout and the user must log in again to reestablish one of the following sessions:

- HTTP session
- HTTPS session
- Console session
- Telnet session
- SSH session

To define the idle session timeout for various types of sessions:

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

STEP 2 Select the timeout for the session from the corresponding drop-down menu. The default value is 10 minutes.

STEP 3 Click **Apply**. The idle session timeout settings are defined, and the Running Configuration is updated.

Ping a Host

Ping is a utility used to test if a remote host can be reached and to measure the round-trip time for packets sent from the switch to a destination device.

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 remote host:

STEP 1 Click **Administration** > **Ping**.

STEP 2 Enter the following information:

- **Host Definition**—Select whether to specify the host by its IP address or name.
- **IP Version**—Select either **Version 4** or **Version 6** if the host is identified by IP address.
- **Host IP Address/Name**—Enter the IP address or hostname of the host to be pinged.
- **Number of Pings**—Select **User Defined** to enter the number of times that the ping operation will be performed, or select **Use Default** to use the default value.

STEP 3 Click **Active Ping** to ping the host. The ping counters and status are displayed.

Using Traceroute

Traceroute discovers the IP routes along which packets were forwarded by sending an IP packet to the target host and back to the switch. The Traceroute page displays each hop between the switch and a target host and the round-trip time to each hop.

To use the Traceroute utility:

STEP 1 Click **Administration** > **Traceroute**.

STEP 2 Enter the following information:

- **Host Definition**—Select whether to specify the host by its IP address or name.
- **Host IP Address/Name**—Enter the IP address or hostname of the host.
- **TTL**—Select **User Defined** to 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 **Apply**.

6

Administration: 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.

The switch supports Simple Network Time Protocol (SNTP) and when enabled, the switch dynamically synchronizes its time with the SNTP server time. The switch operates only as an SNTP client and cannot provide time services to other devices.

This chapter describes how to configure the system time, time zone, and daylight savings time (DST).

It includes the following topics:

- **System Time Options**
- **Configuring System Time**
- **Configuring SNTP Server**
- **Time Range**

System Time Options

System time can be set manually by the user, or dynamically from an SNTP server. If an SNTP server is chosen, the manual time settings are overwritten when communications with the server are established.

As part of the boot process, the switch always configures the time, time zone, and DST. These parameters are obtained from the SNTP, values set manually, or if all else fails, from the factory defaults.

The following methods are available for setting the system time on the switch:

- **Manual**—You must manually set the time.
- **SNTP**—Time can be received from the SNTP time server. SNTP ensures accurate network time synchronization of the switch up to the millisecond by using an SNTP server for the clock source.

NOTE Without synchronized time, accurately correlating log files between devices is difficult, even impossible. We recommend that you use SNTP for the clock source.

Configuring System Time

Use the System Time page to configure the current time, time zone, and the time source.

CAUTION The switch does not have an internal clock that updates this value. If the system time is set manually and the switch is rebooted, the manual time settings must be reentered.

To define system time:

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

The **Actual Time** field displays the current system time and time source currently used by the switch.

STEP 2 Check **Enable** next to the **Main Clock Source (SNTP Servers)** field to use the SNTP source to set the system clock. The system time is obtained from an SNTP

server. To use this feature, you must also add an SNTP server on the SNTP Settings page, as described in the **Configuring SNTP Server** section.

STEP 3 In the **Manual Settings** area, you can set the date and time manually. The local time is used when there is no alternate source of time, such as an SNTP server. You can also click the **here** link to receive the date and time from the PC by using browser information.

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

STEP 4 In the **Time Zone Settings** area, the local time is used via the Time Zone offset.

- **Time Zone Offset**—Select the difference in hours between Universal Time Coordinated (UTC) and the local time. For example, the Time Zone Offset for Paris is UTC +10:00, while the Time Zone Offset for New York is UTC - 5.
- **Time Zone Acronym**—Enter a user-defined name that represents the time zone that you have configured. This acronym appears in the **Actual Time** field.

STEP 5 In the **Daylight Saving Settings** area, select how DST is defined:

- **Daylight Saving**—Check **Enable** to enable Daylight Saving Time.
- **Time Set Offset**—Enter the number of minutes offset from UTC.
- **Daylight Saving Type**—Click one of the following:
  - *USA*—DST will be set according to the dates used in the USA.
  - *European*—DST will be set according to the dates used by the European Union and other countries that use this standard.
  - *By Dates*—DST will be set manually, typically for a country other than the USA or a European country.
  - *Recurring*—DST occurs on the same date every year.

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

- **From**—Enter the day and time that DST starts.
- **To**—Enter the day and time that DST ends.

Selecting *Recurring* allows further customization of the start and stop of DST:

- **From**—Enter the 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**—Enter the date when DST ends each year.

- *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 6 Click **Apply**. The system time is defined, and the Running Configuration is updated.

Configuring SNTP Server

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 DNS servers on the switch and enable Main Clock Source (SNTP Servers) on the System Time page.

To add an SNTP server:

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.
- **SNTP Server Port**—Enter the UDP port number to be specified in the SNTP message headers. By default, the port number is the well-known IANA value of 123.

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.

Absolute Time Range

To define an absolute time range:

STEP 1 Click **Administration > Time Set tings > Time Range**.

The existing time ranges are displayed.

STEP 2 To add a new time range, click **Add**.

STEP 3 Enter the following fields:

- **Time Range Name**—Enter a new time range name.
- **Absolute Starting Time**—To define the start time, enter the following:
  - **Immediate**—Select for the time range to start immediately.
  - **Date, Time**—Enter the date and time that the Time Range begins.
- **Absolute Ending Time**—To define the start time, enter the following:
  - **Infinite**—Select for the time range to never end.
  - **Date, Time**—Enter the date and time that the Time Range ends.

STEP 4 To add a periodic time range, click **Periodic Range.**

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 date and time that the Time Range begins on a periodic basis.
- **Periodic Ending Time**—Enter the date and time that the Time Range ends on a periodic basis.

STEP 5 Click **Apply**.

STEP 6 Click **Time Range** to access the Absolute Time Range.

7

Administration: Diagnostics

This chapter contains information for configuring port mirroring, running cable tests, and viewing optical module status and CPU utilization.

It includes the following topics:

- **Testing Copper Ports**
- **Viewing Optical Module Status**
- **Configuring Port and VLAN Mirroring**
- **Viewing CPU Utilization**

Testing Copper Ports

Use the Copper Test page to perform the integrated cable tests on copper cables.

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. We do not recommend that you run the test on a port that you are using to run the web-based interface, because communications with that device are disrupted.

To test copper cables attached to ports:

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

STEP 2 Select a port on which to run the copper test.

STEP 3 Click **Copper Test**.

The following fields for the test are displayed:

- **Test Results**—Summary of the test results.

- **Cable Length**—Estimated cable length. The cable length is Unknown when the green features are enabled.

  NOTE The estimated cable length for the ports if their links are up or their connected cables are less than 10 meters are used for reference only.

- **Operational Port Status**—Displays whether the port is up or down.

Viewing Optical Module Status

The Optical Module Status page displays the operating conditions reported by the Small Form-factor Pluggable (SFP) transceiver. Some information may not be available for SFPs that do not support the digital diagnostic monitoring standard SFF-8472.

The following FE SFP (100 Mbps) transceivers are supported:

- **MFEBX1**—100BASE-BX-20U SFP transceiver for single-mode fiber, 1310 nm wavelength, supports up to 20 km.
- **MFEFX1**—100BASE-FX SFP transceiver, for multimode fiber, 1310 nm wavelength, supports up to 2 km.
- **MFELX1**—100BASE-LX SFP transceiver, for single-mode fiber, 1310 nm wavelength, supports up to 10 km.

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

- **MGBBX1**—1000BASE-BX-20U SFP transceiver, for single-mode fiber, 1310 nm wavelength, supports up to 40 km.
- **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.

To view the status of optical modules, click **Administration** > **Diagnostics** > **Optical Module Status**.

The following fields are displayed:

- **Port**—Port number on which the SFP is connected.
- **Temperature**—Temperature in Celsius at which the SFP is operating.
- **Voltage**—SFP's operating voltage.
- **Current**—SFP's 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.

Configuring Port and VLAN Mirroring

Port Mirroring is used on a network switch to send a copy of network packets seen on one switch port, multiple switch ports, or an entire VLAN to a network monitoring connection on another port on the switch. Port Mirroring is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system. A network analyzer connected to the monitoring port processes the data packets for diagnosing, debugging, and performance monitoring.

The switch supports up to four mirroring sessions. Each session can be used for local mirroring or remote mirroring purposes. Mirroring does not affect the switching of network traffic on the source ports or VLANs. Each session should have a different destination port. Except for traffic that is required for the mirroring, the destination port can also be used to receive or forward normal traffic.

A packet that is received on a network port 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 switch are mirrored when Transmit (Tx) mirroring is activated.

Mirroring does not guarantee that all traffic from the source ports 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.

NOTE The RSPAN VLAN feature is only applicable for the China switch models.

To configure port and VLAN mirroring:

STEP 1 Click **Administration** > **Diagnostics** > **Port and VLAN Mirroring**.

STEP 2 If your switch supports the RSPAN VLAN feature, enter the following information:

- **RSPAN VLAN**—Check **Enable** to enable RSPAN VLAN mirroring.
- **RSPAN VLAN ID**—Select the VLAN to be mirrored. When you configure a RSPAN mirroring session, you should select this VLAN as the RSPAN VLAN.

STEP 3 Click **Add** to add a SPAN or RSPAN mirroring session.

STEP 4 Enter the following information:

- **Session ID**—Select the identifier for the mirroring session.
- **Session Type**—Select one of the following options:
  - *Local Port Based*—Copies TX, RX, or both TX and RX traffic from each port to the destination port.
  - *Local VLAN Based*—Copies traffic from the local VLAN to the destination port.
  - *RSPAN Source Session*—Utilizes a VLAN to copy traffic from a source port or a source VLAN to another device.
  - *RSPAN Destination Session*—Utilizes a VLAN to copy traffic from a destination port to another device.

STEP 5 If Local Port Based is selected, enter the following information:

- **Destination Port**—Select the analyzer port to where packets are copied. A network analyzer, such as a PC running Wireshark, is connected to this port.
- **Allow Ingress Packets**—Check **Enable** to allow the destination port to send or receive normal packets.
- **Source Port**—Select the source ports from where traffic is mirrored and the type of traffic to be mirrored to the analyzer port. The options are:
  - *Rx Only*—Port mirroring on incoming packets.
  - *Tx Only*—Port mirroring on outgoing packets.
  - *Tx and Rx*—Port mirroring on both incoming and outgoing packets.
  - *N/A*—Traffic from this port is not mirrored.

STEP 6 If Local VLAN Based is selected, enter the following information:

- **Destination Port**—Select the analyzer port to where packets are copied.
- **Allow Ingress Packets**—Check **Enable** to allow the destination port to send or receive normal packets.
- **VLAN**—Select the source VLAN from where traffic is mirrored.

STEP 7 If RSPAN Source Session is selected, enter the following information:

- **RSPAN VLAN**—Select the VLAN to be used to copy traffic to another device. This VLAN should be same as the VLAN defined in the **RSPAN VLAN ID** field.
- **Reflector Port**—Select the port or LAG to be connected to another device.
- **Source Type**—Select **Port** or **VLAN** as the source port or source VLAN.

  If Port is selected, select the source ports from where traffic is mirrored and select the type of traffic to be mirrored to the analyzer port. The options are:

  - *Rx Only*—Port mirroring on incoming packets.
  - *Tx Only*—Port mirroring on outgoing packets.
  - *Tx and Rx*—Port mirroring on both incoming and outgoing packets.
  - *N/A*—Traffic from this port is not mirrored.

  If VLAN is selected, select a source VLAN from where traffic is mirrored.

  - *VLAN*—Select a VLAN as the source VLAN.

STEP 8 If RSPAN Destination Session is selected, enter the following information:

- **RSPAN VLAN**—Select a VLAN to be used to copy traffic to another device. This VLAN should be same as the VLAN defined in the **RSPAN VLAN ID** field.
- **Destination Port**—Select the analyzer port to where packets are copied.
- **Allow Ingress Packets**—Check **Enable** to allow the destination port to send or receive normal packets.

STEP 9 Click **Apply**. The Running Configuration is updated.

Viewing CPU Utilization

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

STEP 1 Click **Administration > Diagnostics > CPU Utilization**.

The CPU Utilization page appears.

The **CPU Input Rate** field displays the rate of input frames to the CPU per second.

The window contains a graph of the CPU utilization. The Y axis is percentage of usage, and the X axis is the sample number.

STEP 2 Ensure that the **CPU Utilization** checkbox is enabled.

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.

STEP 4 STEP 4 Click **Apply**.

8

Administration: Discovery

This chapter provides information for configuring discovery, and includes the following topics:

- Configuring Bonjour
- LLDP and CDP
- Configuring LLDP
- Configuring CDP

Configuring Bonjour

As a Bonjour client, the switch periodically broadcasts Bonjour Discovery protocol packets to directly connected IP subnets, advertising its existence and the services that it provides, for example, HTTP, HTTPS, or Telnet.

The switch can be discovered by a network management system or other third-party applications. By default, Bonjour is enabled on the Management VLAN. The Bonjour console automatically detects the switch and displays it.

Bonjour Discovery can only be enabled globally. It cannot be enabled on a per-port or per-VLAN basis. The switch advertises all the services that have been enabled by the administrator based on the configuration on the TCP/UDP Services page.

When Bonjour Discovery is disabled, the switch stops any service type advertisements and does not respond to requests for service from network management applications.

By default, Bonjour is enabled on all interfaces that are members of the Management VLAN.

To globally enable or disable Bonjour:

STEP 1 Click **Administration** > **Discovery Bonjour**.

STEP 2 Check **Enable** to enable Bonjour Discovery globally on the switch, or uncheck to disable it globally.

STEP 3 Click **Apply**. Bonjour is enabled or disabled on the switch, and the Running Configuration is updated.

LLDP and CDP

Link Layer Discovery Protocol (LLDP) and Cisco Discovery Protocol (CDP) are link layer protocols for directly connected LLDP and CDP-capable neighbors to advertise themselves and their capabilities to each other. By default, the switch sends an LLDP or CDP advertisement periodically to all its interfaces and terminates and processes incoming LLDP and CDP packets as required by the protocols. In LLDP and CDP, advertisements are encoded as TLV (Type, Length, Value) in the packet.

In deployments where the CDP-capable (or LLDP-capable) devices are not directly connected and are separated with CDP-incapable (or LLDP-incapable) devices, the CDP-capable (or LLDP-capable) devices may be able to receive the advertisement from other devices only if the CDP-incapable (or LLDP-incapable) devices flood the CDP (or LLDP) packets they receive. If the CDP-incapable (or LLDP-incapable) devices perform VLAN-aware flooding, then CDP-capable (or LLDP-capable) devices can hear each other only if they are in the same VLAN.

It should be noted that a CDP-capable (or LLDP-capable) device may receive advertisement from more than one device if the CDP-incapable (or LLDP-incapable) devices flood the CDP (or LLDP) packets.

The following are additional points about CDP and LLDP configuration:

- CDP and LLDP can be enabled or disabled globally as well as on each port. The CDP or LLDP capability of a port is relevant only if CDP or LLDP is globally enabled.
- If CDP or LLDP is globally enabled, the switch filters out incoming CDP or LLDP packets from ports that are CDP-disabled or LLDP-disabled.

- If CDP or LLDP is globally disabled, the switch can be configured to discard, VLAN-aware flooding, or VLAN-unaware flooding of all incoming CDP or LLDP packets. VLAN-aware flooding floods an incoming CDP or LLDP packet to the VLAN where the packet is received excluding the ingress port. VLAN-unaware flooding floods an incoming CDP or LLDP packet to all the ports excluding the ingress port. The default is to VLAN-unaware flood CDP or LLDP packets when CDP or LLDP is globally disabled. You can configure the discard or flooding of incoming CDP and LLDP packets from the CDP Properties page and the LLDP Properties page, respectively.
- The CDP and LLDP end devices, such as IP phones, learn the voice VLAN configuration from CDP and LLDP advertisements. By default, the switch is enabled to send out CDP and LLDP advertisement based on the voice VLAN configured on the switch. Refer to the **Configuring Voice VLAN** section for details.

  NOTE CDP or LLDP does not distinguish if a port is in a LAG. If there are multiple ports in a LAG, CDP or LLDP transmit packets on each port without taking into account the fact that the ports are in a LAG.
- The operation of CDP or LLDP is independent of the STP status of an interface.
- If 802.1X port access control is enabled on an interface, the switch will transmit and receive CDP or LLDP packets to and from the interface only if the interface is authenticated and authorized.
- If a port is the target of mirroring, then for CDP or LLDP it is considered down.

Configuring LLDP

LLDP is a protocol that enables network managers to troubleshoot and enhance network management in multivendor 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). The network management system models the topology of the network by querying these MIB databases.

LLDP is a link layer protocol. By default, the switch terminates and processes all incoming LLDP packets as required by the protocol.

The LLDP protocol has an extension called LLDP Media Endpoint Discovery (LLDP MED), which provides and accepts information from media endpoint devices such as VoIP phones and video phones.

Following are examples of actions that can be performed with the LLDP feature in a suggested order:

- Enable LLDP globally (LLDP is enabled by default), and enter LLDP global parameters on the LLDP Properties page, as described in the **Configuring LLDP Properties** section.
- Configure LLDP per port on the Port Settings page, as described in the **Configuring LLDP Port Settings** section. On this page, ports can be configured to receive or transmit LLDP PDUs, and specify which TLVs to advertise.
- Create LLDP MED network policies on the LLDP MED Network Policy page, as described in the **Configuring LLDP MED Network Policy** section.
- Associate LLDP MED network policies and the optional LLDP MED TLVs to the desired ports on the LLDP MED Port Settings page, as described in the **Configuring LLDP MED Port Settings** section.
- View LLDP global information and the LLDP status of each port as described in the **Viewing LLDP Port Status** section.
- View LLDP local information as described in the **Viewing LLDP Local Information** section.
- View LLDP neighbor information as described in the **Viewing LLDP Neighbors Information** section.
- View LLDP statistics of each port as described in the **Viewing LLDP Statistics** section.
- View LLDP overloading information as described in the **Viewing LLDP Overloading** section.

Configuring LLDP Properties

Use the LLDP Properties page to enable LLDP globally and configure general LLDP parameters.

To define LLDP properties:

STEP 1 Click **Administration** > **Discovery LLDP** > **Properties**.

STEP 2 Enter the following information:

- **LLDP Status**—Check **Enable** to enable LLDP on the switch (enabled by default).
- **LLDP Frames Handling**—If LLDP is disabled, select the action to be taken if a packet that matches the selected criteria is received:
  - *Filtering*—Deletes the packet.
  - *Bridging*—(VLAN-aware flooding) Forwards the packet to all VLAN members.
  - *Flooding*—Forwards the packet to all ports.
- **TLV Advertise Interval**—Select **User Defined** to enter the rate in seconds at which LLDP advertisement updates are sent, or select **Use Default** to use the default value (30 seconds).
- **Hold Multiplier**—Select **User Defined** to set 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. You can select **Use Default** to use the default value (4).
- **Reinitializing Delay**—Select **User Defined** to enter the time interval in seconds that passes between disabling and reinitializing LLDP, following an LLDP enable or disable cycle, or select **Use Default** to use the default value (2 seconds).
- **Transmit Delay**—Select **User Defined** to enter the amount of time in seconds that passes between successive LLDP frame transmissions due to changes in the LLDP local systems MIB, or select **Use Default** to use the default value (2 seconds).

STEP 3 In the **Fast Start Repeat Count** field, enter the number of times that LLDP packets are sent when the LLDP MED Fast Start mechanism is initialized. This occurs when a new endpoint device links to the switch. Refer the **Configuring LLDP MED Network Policy** section for more details.

STEP 4 Click **Apply**. The LLDP properties are defined, and the Running Configuration is updated.

Configuring LLDP Port Settings

Use the Port Settings page to activate LLDP per port and enter the TLVs that are sent in the LLDP PDU.

To define the LLDP port settings:

STEP 1 Click **Administration** > **Discovery LLDP** > **Port Settings**.

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

STEP 3 Enter the following information:

- **Interface**—Select the port to be defined.
- **Administrative Status**—Select the LLDP publishing option for the port. The available options are:
  - *Tx Only*—Publishes only but does not discover.
  - *Rx Only*—Discovers but does not publish.
  - *Tx & Rx*—Publishes and discovers.
  - *Disable*—Disables LLDP on the port.
- **Available Optional TLVs**—Select the information to be published by the switch by moving the TLV to the **Selected Optional TLVs** list. The available TLVs contain the following information:
  - *Port Description*—Information about the port, including manufacturer, product name, and hardware and software versions.
  - *System Name*—System's assigned name (in alphanumeric format). The value equals the sysName object.
  - *System Description*—Description of the network entity (in alphanumeric format). This includes the system's name and versions of the hardware, operating system, and networking software supported by the switch. The value equals the sysDescr object.

- *System Capabilities*—Primary functions of the switch, and whether or not these functions are enabled in the switch. 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.
- *802.3 MAC-PHY*—Duplex and bit rate capability and the current duplex and bit rate settings of the sending device. It also indicates whether the current settings are due to auto-negotiation or manual configuration.
- *802.3 Link Aggregation*—Whether the link (associated with the port on which the LLDP PDU is transmitted) can be aggregated. It also indicates whether the link is currently aggregated, and if so, provides the aggregated port identifier.
- *802.3 Maximum Frame Size*—Maximum frame size capability of the MAC/PHY implementation.
- *Management IP Address*—Management IP address of the switch.

STEP 4 Click **Apply**. The LLDP port settings are modified, and the Running Configuration is updated.

Configuring LLDP MED Network Policy

LLDP Media Endpoint Discovery (LLDP MED) is an extension of LLDP that provides the following additional capabilities to support media endpoint devices. Some of the features of the LLDP MED network policy are:

- Enables the advertisement and discovery of network policies for real-time applications such as voice and/or video.
- Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Emergency Call Service (E-911) by using IP Phone location information.

NOTE The switch automatically advertises the policy according to user configuration; however, the user must also manually configure the switch to use that policy.

An 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, will be included into the outgoing LLDP packets to the attached LLDP media endpoint device. The media endpoint device should send its traffic as specified in the network policy that it receives.

Network policies are associated with ports on the LLDP MED Port Settings page. An administrator can manually configure one or more network policies and the ports 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 ports.

To define LLDP MED network policies:

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

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 switch.

STEP 3 Click **Apply**.

STEP 4 Click **Add** to add an LLDP MED network policy.

STEP 5 Enter the following information:

- **Network Policy Number**—Select the number of the policy to be created.
- **Application**—Select the type of application (type of traffic) from the list for which the network policy is being defined:
  - Voice
  - Voice Signaling
  - Guest Voice
  - Guest Voice Signaling
  - Softphone Voice
  - Video Conferencing
  - Streaming Video
  - Video Signaling
- **VLAN ID**—Enter the VLAN ID to which the traffic should 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.

- **DSCP Value**—Select the DSCP value to associate with application data sent by neighbors. This informs them how they should mark the application traffic that they send to the switch.

STEP 6 Click **Apply**. The LLDP MED network policy is defined, and the Running Configuration is updated.

STEP 7 Associate the network policy with a port as described in the **Configuring LLDP MED Port Settings** section.

Configuring LLDP MED Port Settings

Use the LLDP MED Port Settings page to select the network policies, configured on the LLDP MED Network Policy page, to be advertised on the port, and select the LLDP MED TLVs to be sent inside the LLDP PDU.

To configure LLDP MED on each port:

STEP 1 Click **Administration** > **Discovery LLDP** > **LLDP MED Port Settings**.

STEP 2 To associate the LLDP MED network policy to a port, select a port and click **Edit**.

STEP 3 Enter the following information:

- **Interface**—Select a port to be configured.
- **LLDP MED Status**—Enable or disable LLDP MED on this port.
- **Available Optional TLVs**—Select the TLVs that can be published by the switch, by moving them to the **Selected Optional TLVs** list.
- **Available Network Policies**—Select the LLDP MED policies that will be published by LLDP, by moving them to the **Selected Network Policies** list. These policies were created on the LLDP MED Network Policy page.

  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 4 Click **Apply**. The LLDP MED port settings are modified, and the Running Configuration is updated.

STEP 5 Click **LLDP Local Information Detail** to see the details of the LLDP and LLDP MED TLVs sent to the neighbor.

Viewing LLDP Port Status

The LLDP Port Status page displays the LLDP global information, as well as the LLDP status per port.

To view the LLDP port status:

STEP 1 Click **Administration** > **Discovery LLDP** > **LLDP Port Status**.

The following fields are displayed:

- **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 switch is displayed.
- **System Name**—Name of the switch.
- **System Description**—Description of the switch (in alphanumeric format).
- **Supported System Capabilities**—Primary functions of the device, such as Bridge, WLAN AP, or Router.
- **Enabled System Capabilities**—Primary enabled functions of the device.
- **Port ID Subtype**—Type of the port identifier that is shown.

The following LLDP information for each port is displayed:

- **Interface**—Port identifier.
- **LLDP Status**—LLDP publishing option.
- **LLDP MED Status**—Where LLDP MED is enabled or disabled on the port.
- **Local PoE**—(Only applicable for PoE models) Local PoE information advertised.
- **Remote PoE**—(Only applicable for PoE models) PoE information advertised by the neighbor.

- **# of neighbors**—Number of neighbors discovered.
- **Neighbor Capability of 1st Device**—Displays the primary enabled device functions of the neighbor, for example, Bridge or Router.

STEP 2 Click **LLDP Local Information Detail** to see the details of the LLDP and LLDP MED TLVs sent to the neighbor.

STEP 3 Click **LLDP Neighbor Information Detail** to see the details of the LLDP and LLDP MED TLVs received from the neighbor.

Viewing LLDP Local Information

To view the LLDP local port status advertised on a port:

STEP 1 Click **Administration > Discovery LLDP > LLDP Local Information**.

STEP 2 Select the desired port from the **Port** drop-down menu.

The following fields are displayed:

Global

- **Chassis ID Subtype**—Type of chassis ID, such as the MAC address.
- **Chassis ID**—Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the switch is displayed.
- **System Name**—Name of switch.
- **System Description**—Description of the switch (in alphanumeric format).
- **Supported System Capabilities**—Primary functions of the device, such as Bridge, WLAN AP, or Router.
- **Enabled System Capabilities**—Primary enabled functions 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 and software versions.

Management Address

Displays the table of addresses of the local LLDP agent. Other remote managers can use this address to obtain information related to the local device. The address consists of the following elements:

- **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.
- **Auto-Negotiation Enabled**—Port speed auto-negotiation active status.
- **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 supported on the port.

- **Current Capabilities**—MED capabilities enabled on the port.
- **Device Class**—LLDP MED endpoint device class.
- **PoE Device Type**—(Only applicable for PoE models) Port PoE type, for example, powered.
- **PoE Power Source**—(Only applicable for PoE models) Port power source.
- **PoE Power Priority**—(Only applicable for PoE models) Port power priority.
- **PoE Power Value**—(Only applicable for PoE models) Port 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

- **Civic**—Street address.
- **Coordinates**—Map coordinates: latitude, longitude, and altitude.
- **ECS ELIN**—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 for which the network policy is defined. The possible field values are:
  - *Tagged*—Indicates the network policy is defined for tagged VLANs.
  - *Untagged*—Indicates the network policy is defined for untagged VLANs.
- **User Priority**—Network policy user priority.
- **DSCP**—Network policy DSCP.

STEP 3 Click **LLDP Port Status Table** to display the details of LLDP port status in a table.

Viewing LLDP Neighbors Information

The LLDP Neighbor page displays information that was received using the LLDP protocol 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:

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 switch.
- **Time to Live**—Time interval in seconds after which the information for this neighbor is deleted.

STEP 3 Click **Detail** to display the details of LLDP port status in a table.

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

Viewing LLDP Statistics

The LLDP Statistics page displays LLDP statistical information per port.

To view the LLDP statistics:

STEP 1 Click **Administration** > **Discovery LLDP** > **LLDP Statistics**.

The following fields are displayed for each port:

- **Interface**—Port identifier.
- **Tx Frames Total**—Total number of transmitted frames.
- **Rx Frames Total**—Number of received frames.
- **Rx Frames Discarded**—Total number of received frames that were discarded.
- **Rx Frames Errors**—Total number of received frames with errors.
- **Rx TLVs Discarded**—Total number of received TLVs that were discarded.
- **Rx TLVs Unrecognized**—Total number of received TLVs that were unrecognized.
- **Neighbor's Information Deletion Count**—Number of neighbor age outs on the port.

STEP 2 Click **Refresh** to refresh the LLDP statistics.

Viewing 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 a port.

The LLDP Overloading page displays the number of bytes of LLDP/LLDP MED information, the number of available bytes for additional LLDP information, and the overloading status of each port.

To view LLDP overloading information:

STEP 1 Click **Administration** > **Discovery LLDP** > **LLDP Overloading**.

The following fields are displayed:

- **Interface**—Port identifier.
- **Total Bytes In-Use**—Total number of bytes of LLDP information in each packet.
- **Available Bytes Left** —Total number of available bytes left for additional LLDP information in each packet.
- **Status**—If TLVs are transmitted, or if they are overloaded.

STEP 2 Select a port and click **Details**.

The following fields are displayed:

- **LLDP Mandatory TLVs**
  - *Size (Bytes)*—Total mandatory TLV byte size.
  - *Status*—If the mandatory TLV group is transmitting, or if the TLV group was overloaded.
- **LLDP MED Capabilities**
  - *Size (Bytes)*—Total LLDP MED capabilities packets byte size.
  - *Status*—Whether the LLDP MED capabilities packets were sent or they were overloaded.
- **LLDP MED Location**
  - *Size (Bytes)*—Total LLDP MED location packets byte size.
  - *Status*—Whether the LLDP MED location packets were sent or they were overloaded.
- **LLDP MED Network Policy**
  - *Size (Bytes)*—Total LLDP MED network policies packets byte size.
  - *Status*—If the LLDP MED network policies packets were sent, or if they were overloaded.
- **LLDP MED Expanded 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 were sent, or if they were overloaded.

- **802.3 TLVs**
  - *Size (Bytes)*—Total LLDP 802.3 TLVs packets byte size.
  - *Status*—If the LLDP 802.3 TLVs packets were sent, or if they were overloaded.
- **LLDP Optional TLVs**
  - *Size (Bytes)*—Total LLDP optional TLVs packets byte size.
  - *Status*—If the LLDP optional TLVs packets were sent, or if they were overloaded.
- **LLDP MED Inventory**
  - *Size (Bytes)*—Total LLDP MED inventory TLVs packets byte site.
  - *Status*—If the LLDP MED inventory packets were sent, or if they were overloaded.
- **802.1 TLVs**
  - *Size (Bytes)*—Total LLDP 802.1 TLVs packets byte size.
  - *Status*—If the LLDP 802.1 TLVs packets were sent, or if they were overloaded.
- **Total**
  - *Total (Bytes)*—Total number of bytes of LLDP information in each packet.
  - *Available Bytes Left*—Total number of available bytes left for additional LLDP information in each packet.

Configuring CDP

Similar to LLDP, 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.

This section describes how to configure CDP and includes the following topics:

- **Configuring CDP Properties**
- **Configuring CDP Port Settings**
- **Viewing CDP Local Information**
- **Displaying CDP Neighbor Information**
- **Viewing CDP Statistics**

Configuring CDP Properties

Use the CDP Properties page to globally enable CDP on the switch and configure general CDP parameters.

To define CDP properties:

STEP 1 Click **Administration** > **Discovery CDP** > **Properties**.

STEP 2 Enter the following information:

- **CDP Status**—Check **Enable** to globally enable CDP on the switch.
- **CDP Frames Handling**—If CDP is disabled, 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**—Check **Enable** to enable the switch to advertise the voice VLAN in CDP on all ports that are CDP-enabled, and are members of the voice VLAN.

- **CDP Mandatory TLVs Validation**—Check **Enable** to discard incoming CDP packets not containing the mandatory TLVs and the invalid error counter is incremented.
- **CDP Version**—Select the version of CDP to use.
- **CDP Hold Time**—Select **User Defined** to enter the amount of time in seconds that CDP packets are held before the packets are discarded, measured in multiples of the TLV Advertise Interval. For example, if the TLV Advertise Interval is 30 seconds, and the Hold Multiplier is 4, then the LLDP packets are discarded after 120 seconds. You can also select **Use Default** to use the default time (180 seconds).
- **CDP Transmission Rate**—Select **User Defined** to enter the rate in seconds at which CDP advertisement updates are sent, or select **Use Default** to use the default rate (60 seconds).
- **Device ID Format**—Select the format of the device ID (MAC address, serial number, or host name).
- **Source Interface**—Select **User Defined** to use the IP address of the interface (defined in the **Interface** field) in the address TLV, or select **Use Default** to use the IP address of the outgoing interface.
- **Interface**—If *User Defined* was selected for **Source Interface**, select the interface.
- **Syslog Voice VLAN Mismatch**—Check **Enable** 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 **Enable** 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 **Enable** 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, and the Running Configuration is updated.

Configuring CDP Port Settings

Use the Port Settings page to enable or disable CDP per port. Notifications can also be triggered when there are conflicts with CDP neighbors. The conflict can be Voice VLAN data, Native VLAN, or Duplex.

To define the CDP port settings:

STEP 1 Click **Administration** > **Discovery CDP** > **Port Settings**.

The following fields are displayed:

- **Interface**—Port identifier.
- **CDP Status**—CDP publishing option for the port.
- **Reporting Conflicts with CDP Neighbors**—Displays the status of the reporting options (Voice VLAN/Native VLAN/Duplex) that are enabled or disabled on the Edit page.
- **No. of Neighbors**—Number of neighbors detected.

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

STEP 3 Enter the following information:

- **Interface**—Select the port to be defined.
- **CDP Status**—Check **Enable** to enable the CDP publishing option for the port.

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

- **Syslog Voice VLAN Mismatch**—Check **Enable** 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 **Enable** 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 **Enable** to send a SYSLOG message when duplex information mismatch is detected. This means that the duplex information in the incoming frame does not match what the local device is advertising.

STEP 4 Click **Apply**. The CDP port settings are modified, and the Running Configuration is updated.

Viewing CDP Local Information

The CDP Local Information page displays information that is advertised by the CDP protocol about the local device.

To view the CDP local information:

STEP 1 Click **Administration** > **Discovery CDP** > **CDP Local Information**.

STEP 2 Select a local port, and the following fields are displayed:

- **CDP State**—Displays whether CDP is enabled or disabled on the port.
- **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.
- **Address TLV**
  - *Address(s)*—IP addresses (advertised in the device address TLV).
- **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/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, meaning that the host/server from which the packet is received is trusted to mark the packets itself. In this case, packets received on such a port are not remarked. Disabled indicates that the port is not trusted in which case, the following field is relevant.
- **CoS for Untrusted Ports TLV**
  - *CoS/802.1p for Untrusted Ports*—If Extended Trust is disabled on the port, this field displays the Layer 2 CoS value, which is 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 TLV** (Only applicable for PoE models)
  - *Request ID*—(Only applicable for PoE models) Last power request ID received echoes the Request-ID field last received in a Power Requested TLV. It is 0 if no Power Requested TLV was received since the interface last transitioned to Up.
  - *Power Management ID*—(Only applicable for PoE models) Value incremented by 1 (or 2, to avoid 0) each time when the Available Power or Management Power Level fields change value. A Power Requested TLV is received with a Request-ID field which is different from the last-received set (or when the first value is received). The interface transitions to Down.
  - *Available Power*—(Only applicable for PoE models) Amount of power consumed by port.

- *Management Power Level*—(Only applicable for PoE models) Display the supplier's request to the powered device for its Power Consumption TLV. The switch always displays “No Preference” in this field.

Displaying CDP Neighbor Information

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

To view the CDP neighbor information:

STEP 1 Click **Administration** > **Discovery CDP** > **CDP Neighbor Information**.

The following fields are displayed:

- **Device ID**—Neighbor’s 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 2 Select a neighbor device, and click **Detail**.

The following fields about the neighbor are displayed:

- **Device ID**—Identifier of the neighboring device ID.
- **Local Interface**—Interface number of port through which frame arrived.
- **Advertisement Version**—Version of CDP.
- **Time to Live**—Time interval (in seconds) after which the information for this neighbor is deleted.

- **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.
- **Platform**—Identifier of the neighbor's platform.
- **Neighbor Interface**—Interface number of the neighbor through which frame arrived.
- **Native VLAN**—Neighbor's native VLAN.
- **Duplex**—Whether neighbors interface is half or full duplex.
- **Addresses**—Neighbor's addresses.
- **Power Drawn**—(Only applicable for PoE models) Amount of power consumed by neighbor on the interface.
- **Version**—Neighbor's software version.

STEP 3 Click **Clear Table** to disconnect all connected neighbor devices from CDP.

STEP 4 Click **Refresh** to refresh the CDP neighbor information.

Viewing CDP Statistics

The CDP Statistics page displays information regarding CDP frames that were sent or received from a port.

CDP statistics for a port are only displayed if CDP is enabled globally and on the port.

To view CDP statistics:

STEP 1 Click **Administration** > **Discovery CDP** > **CDP Statistics**.

The following fields are displayed:

- **Packets Received**—Displays the counters for various types of packets received per interface.
  - *Version 1*—Number of CDP version 1 packets received.
  - *Version 2*—Number of CDP version 2 packets received.
  - *Total*—Total number of CDP packets received.

- **Packets Transmitted**—Displays the counters for various types of packets transmitted per interface.
  - *Version 1*—Number of CDP version 1 packets transmitted.
  - *Version 2*—Number of CDP version 2 packets transmitted.
  - *Total*—Total number of CDP packets transmitted.
- **CDP Error Statistics**—Displays the CDP error counters.
  - *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 could not be stored in cache because of lack of room.

STEP 2 Select an interface and click **Clear Interface Counters** to clear the CDP statistics counters for the selected interface.

STEP 3 Click **Clear All Interfaces Counters** to clear the CDP statistics counters for all interfaces.

STEP 4 Click **Refresh** to refresh the CDP statistics counters.

9

Port Management

This chapter describes port configuration, link aggregation, and the Energy Efficient Ethernet feature.

It includes the following topics:

- Port Management Workflow
- Configuring Basic Port Settings
- Configuring Error Recovery Settings
- Loopback Detection
- Configuring Link Aggregation
- Configuring Energy Efficient Ethernet

Port Management Workflow

To configure ports, perform the following actions:

STEP 1 Configure basic port parameters on the Port Settings page, as described in the **Configuring Basic Port Settings** section.

STEP 2 Enable or disable the error-disabled ports to recover from specific causes and manually activate the suspended ports on the Error Recovery Settings page, as described in the **Configuring Error Recovery Settings** section.

STEP 3 Enable or disable the Link Aggregation Control (LAG) protocol, and configure the potential member ports to the desired LAGs on the LAG Management page, as described in the **Configuring Link Aggregation** section. By default, all LAGs are empty.

STEP 4 Configure the Ethernet parameters, such as speed and auto-negotiation for the LAGs on the LAG Settings page, as described in the **Configuring LAG Settings** section.

STEP 5 Configure the LACP parameters for the ports that are members or candidates of a dynamic LAG on the LACP page, as described in the **Configuring LACP** section.

STEP 6 Configure 802.3 Energy Efficient Ethernet per port on the Energy Efficient Ethernet > Port Settings page, as described in the **Configuring Energy Efficient Ethernet** section.

STEP 7 If PoE is supported and enabled for the switch, configure the switch as described in the **Power over Ethernet** chapter.

Configuring Basic Port Settings

Use the Port Settings page to configure the port settings globally or per port.

NOTE NOTE The Disable Port LEDs feature saves power consumed by device LEDs. Because the devices are often in an unoccupied room, having these LEDs lit is a waste of energy. The feature enables you to disable the port LEDs (for link, speed, and PoE) when they are not required, and to enable the LEDs if they are needed (debugging, connecting additional devices etc.). On the System Summary page, the LEDs that are displayed on the device board pictures are not affected by disabling the LEDs.

To configure the port settings:

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

STEP 2 Select **Port LEDs** to enable the port LEDs.

When these are disabled, they do not display link status, activity, etc.

STEP 3 Check **Enable** beside the **Jumbo Frames** field to support packets of up to 10,000 bytes in size. If Jumbo Frames is not enabled (default), the switch supports packet size up to 1522 bytes.

STEP 4 Click **Apply**. The global port setting is defined, and the Running Configuration is updated.

STEP 5 To update the settings of a port, select the desired port and click **Edit.**

STEP 6 Enter the following information:

- **Interface**—Select the port to be modified.
- **Port Description**—Enter the port user-defined name or comment.

- **Port Type**—Displays the port type.
- **Administrative Status**—Select whether the port should be operational (Up) or nonoperational (Down) when the switch is rebooted.
- **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. If a time range is not yet defined, click Edit to go to the Time Range page.
- **Time Range Name**—Select the profile that specifies the time range.
- **Operational Time-Range State**—Displays whether the time range is currently active or inactive.
- **Operational Status**—Displays the current port connection status.
- **Auto Negotiation**—Check **Enable** to enable auto-negotiation on the port. Auto-negotiation enables a port to advertise its transmission rate, duplex mode, and flow control abilities to other devices.
- **Operational Auto Negotiation**—Displays the current auto-negotiation status on the port.
- **Administrative Port Speed**—Select the configured rate for the port. The port type determines the available speed setting options. You can designate Administrative Port 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. The possible options are:
  - *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.
- **Operational Duplex Mode**—Displays the port's current duplex mode that is the result of negotiation.
- **Auto Advertisement Speed**—Select the speed capability to be advertised by the port. The options are:
  - *All Speed*—All port speed settings can be accepted.

- *10M*—10 Mbps speed.
- *100M*—100 Mbps speed.
- *10M/100M*—10 and 100 Mbps speeds.
- *1000M*—1000 Mbps speed.

- **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.
- **Operational Advertisement**—Displays the capabilities currently published to the port's neighbor to start the negotiation process. The possible options are those specified in the **Auto Advertisement Speed** and **Auto Advertisement Duplex** fields.
- **Back Pressure**—Check **Enable** to enable the Back Pressure mode on the port (used with Half Duplex mode) to slow down the packet reception speed when the switch is congested. It 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).
- **Current Flow Control**—Displays the current status of 802.3X flow control.
- **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.

- **Member in LAG**—If the port is a member of a LAG, the LAG number appears; otherwise this field is left blank.

STEP 7 Click **Apply**. The port settings are modified, and the Running Configuration is updated.

Configuring Error Recovery Settings

Use the Error Recovery Settings page to globally set the automatic recovery interval, and disable or enable the error-disabled port to recover from specific causes. You can also manually reactivate the suspended ports.

To configure error recovery settings:

STEP 1 Click **Port Management** > **Error Recovery Settings**.

STEP 2 Enter the following global port settings:

- **Automatic Recovery Interval**—Enter the time in seconds to recover from the specified error-disabled state. The same interval is applied to all causes. The default interval is 300 seconds.
- **Automatic ErrDisable Recovery**—Enable or disable the error-disabled port to recover from specific causes. The available causes are:
  - *802.1x Single Host Violation*—Check **Enable** to enable the timer to recover from the 802.1x Single Host Violation causes.
  - *ACL*—Check **Enable** to enable the timer to recover from the ACL causes.
  - *ARP Inspection*—Check **Enable** to the timer to recover from the ARP inspection causes.
  - *BPDU Guard*—Check **Enable** to enable the timer to recover from the BPDU Guard cause.
  - *Broadcast Flood*—Check **Enable** to enable the timer to recover from the Broadcast flood cause.

- *DHCP Rate Limit*—Check **Enable** to enable the timer to recover from the DHCP rate limit causes.
- *Loopback Detection*—Check **Enable** to enable the timer to recover from the Loopback Detection causes.
- *PoE*—(Only applicable for PoE models) Check **Enable** to enable the timer to recover from the Power over Ethernet (PoE) causes.
- *Port Security*—Check **Enable** to enable the timer to recover from the port security causes.
- *Self Loop*—Check **Enable** to enable the timer to recover from the selfloop cause.
- *Unicast Flood*—Check **Enable** to enable the timer to recover from the Unicast flood causes.
- *Unknown Multicast Flood*—Check **Enable** to enable the timer to recover from the unknown Multicast flood causes.

STEP 3 Click **Apply**. The error recovery settings are modified, and the Running Configuration is updated.

STEP 4 The **Suspended (errDisabled) Interface Table** displays a list of suspended ports. To manually reactivate a suspended port, select the desired port, and click **Reactivate**.

Loopback Detection

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.

The following loop cases can be detected by the Loopback Detection protocol:

- Shorted wire—Port that loop backs all receiving traffic.

- Direct multi-ports loop—Switch is connected to another switch with more than one port and STP is disabled.
- LAN segment loop—Switch is connected with one or more ports to a LAN segment that has loops.

How LBD Works

LBD protocol periodically broadcast loopback detection packets. A switch detects a loop when it receives its own LBD packets.

The following conditions must be true for a port to be LBD active:

- LBD is globally enabled.
- LBD is enabled on the port.
- Port operational status is up.
- Port is in STP forwarding/disable state (MSTP instance forwarding state, instance 0).

LBD frames are transmitted on the highest priority queue on LBD active ports (in case of LAGs, the LBD is transmitted on every active port member in LAG).

When a loop is detected, the switch performs the following actions:

- Sets the receiving ports or LAGs to Error Disable state.
- Issues an appropriate SNMP trap.
- Generates an appropriate SYLOG message.

Configuring Loopback Detection

Default Settings and Configuration

Loopback detection is not enabled by default.

Detection interval is 30 seconds.

Interactions with Other Features

If STP is enabled on a port on which Loopback Detection is enabled, the port must be in STP forwarding state.

Configuring LBD Workflow

To enable and configure LBD:

STEP 1 Enable Loopback Detection system-wide in the Loopback Detection Settings page.

STEP 2 Enable Loopback Detection on access ports in the Loopback Detection Settings page.

STEP 3 Enable Auto-Recovery for Loopback Detection in the Error Recovery Settings page.

To configure Loopback Detection:

STEP 1 Click **Port Management > Loopback Detection Settings**.

STEP 2 Select **Enable** in the **Loopback Detection** global field to enable the feature.

STEP 3 Enter the Detection Interval. This is the interval between transmissions 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.

STEP 6 Select the ports or LAGs on which LBD is to be enabled and click **Edit**.

STEP 7 Select **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.

Configuring Link Aggregation

Link Aggregation Control Protocol (LACP) is part of an IEEE specification (802.3az) that allows you to bundle several physical ports together to form a single logical channel. Link aggregation optimizes port usage by linking multiple ports together to form a Link Aggregation Group (LAG). LAGs multiply the bandwidth, increase port flexibility, and provide link redundancy between two devices.

Two types of LAGs are supported:

- **Static**—A LAG is static if the LACP is disabled. A group of ports assigned to a static LAG are always active members. After a LAG is manually created, the LACP option cannot be added or removed, until the LAG is edited and a member is removed (which can be added prior to applying), then the LACP button become available for editing.
- **Dynamic**—A LAG is dynamic if LACP is enabled on it. A 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 the link aggregation features and includes the following topics:

Load Balancing

Traffic forwarded to a LAG is load-balanced across the active member ports, which achieves an effective bandwidth close to the aggregate bandwidth of all the active member ports of the LAG.

Traffic load balancing over the active member ports of a LAG is managed by a hash-based distribution function that distributes Unicast and Multicast traffic based on Layer 2 packet header information.

The switch supports two modes of load balancing:

- **By MAC Addresses**—Based on the destination and source MAC addresses of all packets.
- **By IP and MAC Addresses**—Based on the destination/source IP addresses, and destination/source MAC addresses for all packets.

LAG Management

Active member ports in a LAG are defined statically by explicit user assignment or are dynamically selected by the LACP. The LACP selection process selects the active member ports for the LAG after exchanging LACP information between the local and remote devices.

In general, a LAG is treated by the system as a single logical port. In particular, the LAG has port attributes similar to a regular port, such as state and speed.

The switch supports eight LAGs. Every LAG has the following characteristics:

- All ports in a LAG must be of the same media type.
- Ports in a LAG must not be assigned to another LAG.
- No more than 8 ports are assigned to a static LAG and no more than 16 ports can be candidates for a dynamic LAG.
- When a port is added to a LAG, the configuration of the LAG applies to the port. When the port is removed from the LAG, its original configuration is reapplied.
- Protocols, such as Spanning Tree, consider all the ports in the LAG to be one port.
- All the ports in the LAG must have the same 802.1p priority.

By default, ports are not members of a LAG and are not candidates to become part of a LAG.

Static and Dynamic LAG Workflow

LACP cannot be enabled for a static LAG that has members. It can only be enabled after the static LAG is edited and all members are removed.

To configure a static LAG, perform the following actions:

STEP 1 Disable LACP on the LAG to make it static. Assign up to eight member ports to the static LAG by selecting and moving the ports from the **Port List** to the **LAG Members** list on the LAG Management page. See **Configuring LAG Management** for more information.

STEP 2 Configure the LAG speed and flow control on the LAG Settings page. See **Configuring LAG Settings** for more information.

To configure a dynamic LAG, perform the following actions:

STEP 1 Enable LACP on the LAG. Assign up to 16 candidates ports to the dynamic LAG by selecting and moving the ports from the **Port List** to the **LAG Members** List on the LAG Management page. See **Configuring LAG Management** for more information.

STEP 2 Configure the LAG speed and flow control on the LAG Settings page. See **Configuring LAG Settings** for more information.

STEP 3 Configure the LACP parameters of the ports in the LAG on the LACP page. See **Configuring LACP** for more information.

Configuring LAG Management

Use the LAG Management page to configure the global and per LAG settings.

To define the load balancing algorithm and LAG membership:

STEP 1 Click **Port Management** > **Link Aggregation** > **LAG Management**.

STEP 2 In the **Load Balance Algorithm** area, select one of the following load balancing algorithms:

- **MAC Address**—Performs load balancing by source and destination MAC addresses on all packets.

- **IP/MAC Address**—Performs load balancing by the source/destination IP addresses and by the source or destination MAC addresses on all packets.

STEP 3 Click **Apply**. The load balancing algorithm is defined, and the Running Configuration is updated.

STEP 4 To define the member or candidate ports in a LAG, select the desired LAG and click **Edit**.

STEP 5 Enter the following information:

- **LAG**—Select the LAG to be defined.
- **LAG Name**—Enter the name of the LAG.
- **LACP**—Check **Enable** to enable LACP on the selected LAG. This makes it a dynamic LAG. This field can only be enabled after moving at least a port to the LAG in the next field.
- **LAG Members**—Move those ports that are to be assigned to the LAG from the **Port List** to the **LAG Members** list. Up to 8 ports per static LAG can be assigned, and 16 ports can be assigned to a dynamic LAG.

STEP 6 Click **Apply**. The LAG membership is defined, and the Running Configuration is updated.

Configuring LAG Settings

Use the LAG Settings page to configure the LAG settings.

To configure the LAG settings:

STEP 1 Click **Port Management** > **Link Aggregation** > **LAG Settings**.

STEP 2 Select a LAG, and click **Edit**.

STEP 3 Enter the following information:

- **LAG**—Select the LAG to be configured.
- **LAG Type**—Displays the port type that comprises the LAG.
- **Description**—Enter the name of the LAG.
- **Administrative Status**—Set the LAG to operational (Up) or nonoperational (Down).

- **Operational Status**—Displays whether the LAG is currently operating.
- **Auto Negotiation**—Enables or disables auto-negotiation on the LAG. Auto-negotiation is a protocol between two link partners that enables a LAG to advertise its transmission rate and flow control to its partner (the flow control is disabled by default). We recommend that you keep auto-negotiation enabled on both sides of an aggregate link, or disabled on both sides, while ensuring that link speeds are identical.
- **Operational Auto Negotiation**—Displays the current auto-negotiation setting.
- **Administrative Port Speed**—Select the LAG speed.
- **Operational LAG Speed**—Displays the current speed at which the LAG is operating.
- **Auto Advertisement Speed**—Select the speed capability to be advertised by the LAG. The options are:
  - *All Speed*—All port speed settings can be accepted.
  - *10M*—10 Mbps speed.
  - *100M*—100 Mbps speed.
  - *10M/100M*—10 Mbps and 100 Mbps speeds.
  - *1000M*—1000 Mbps speed.
- **Operational Advertisement**—Displays the current advertisement status. The LAG advertises its capabilities to its neighbor LAG to start the negotiation process. The possible values are those specified in the **Auto Advertisement Speed** field.
- **Back Pressure**—Check **Enable** to enable the Back Pressure mode on the LAG (used with Half Duplex mode) to slow down the packet reception speed when the switch is congested.
- **Flow Control**—Enables or disables Flow Control, or enables the auto-negotiation of Flow Control on the LAG.
- **Current Flow Control**—Displays the current Flow Control setting.
- **Protected Port**—Check **Enable** to make the LAG a protected port for Layer 2 isolation.

STEP 4 Click **Apply**. The LAG settings are defined, and the Running Configuration is updated.

Configuring LACP

A dynamic LAG is LACP-enabled, and LACP runs on every candidate port defined in the LAG.

LACP Priority and Rules

LACP system priority and LACP port priority are both used to determine which candidate ports become active member ports in a dynamic LAG.

The selected candidate ports of the LAG are all connected to the same remote device. Both the local and remote switches have a LACP system priority.

The following algorithm is used to determine whether LACP port priorities are taken from the local or remote device: the local LACP System Priority is compared to the remote LACP System Priority. The device with the lowest priority controls candidate port selection to the LAG. If both priorities are the same, the local and remote MAC addresses are compared. The priority of the device with the lowest MAC address controls candidate port selection to the LAG.

A dynamic LAG can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. When there are more than eight ports in the dynamic LAG, the switch on the controlling end of the link uses port priorities to determine which ports are bundled into the LAG and which ports are put in hot-standby mode. Port priorities on the other device (the non-controlling end of the link) are ignored.

The following are additional rules used to select the active or standby ports in a dynamic LACP:

- Any link operating at a different speed from the highest-speed active member or operating at half-duplex becomes standby. All the active ports in a dynamic LAG operate at the same baud rate.
- If the port LACP priority of the link is lower than that of the currently active link members, and the number of active members is already at the maximum number, the link becomes inactive, and placed in standby mode.

LACP With No Link Partner

In order for LACP to create a LAG, the ports on both link ends should be configured for LACP, which means that the ports send LACP PDUs and handle received PDUs.

However, there are cases when one link partner is temporarily not configured for LACP. One example for such case is when the link partner is on a device, that is in the process of receiving its configuration using the auto-config protocol. This device's ports are not yet configured to LACP. If the LAG link cannot come up, the device cannot ever become configured. A similar case occurs with dual-NIC network-boot computers (for example, PXE), which receive their LAG configuration only after they boot up.

When several LACP-configured ports are configured, and the link comes up in one or more ports but there are no LACP responses from the link partner for those ports, the first port that had link up is added to the LACP LAG and becomes active (the other ports become non-candidates). In this way, the neighbor device can, for example, get its IP address using DHCP and get its configuration using auto-configuration.

Configuring LACP Parameters

Use the LACP page to configure the candidate ports for the LAG and to configure the LACP parameters per port.

LACP timeout is a per-port parameter, and is the time interval between the sending and receiving of consecutive LACP PDUs. With all factors equal, when the LAG is configured with more candidate ports than the maximum number of active ports allowed (8), the switch selects ports as active from the dynamic LAG 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:

STEP 1 Click **Port Management** > **Link Aggregation** > **LACP**.

STEP 2 In the **LACP System Priority** field, enter the global LACP priority value for all ports.

STEP 3 Click **Apply**. The LACP system priority is defined, and the Running Configuration is updated.

STEP 4 To edit the LACP settings for a specific port, select the desired port, and click **Edit**.

STEP 5 Enter the following information:

- **Interface**—Select the port to be defined.
- **LACP Port Priority**—Enter the LACP priority value for the selected port.
- **LACP Timeout**—Select long or short timeout for neighbor LACP PDUs, which will affect the periodic transmissions of neighbor LACP PDUs at either a slow (Long) or fast (Short) transmission rate.

STEP 6 Click **Apply**. The Running Configuration is updated.

Configuring Energy Efficient Ethernet

Energy Efficient Ethernet (EEE) is designed to save power when there is no traffic on the link. With Energy Efficient Ethernet, power is reduced when the port is up, but there is no traffic on it.

Energy Efficient Ethernet reduces overall power usage in Energy-Detect mode. Energy Efficient Ethernet is defined per port, regardless of their LAG membership.

To enable Energy Efficient Ethernet on a port:

STEP 1 Click **Port Management** > **Energy Efficient Ethernet** > **Port Settings**.

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

- **Interface**—Select the port to be configured.
- **Energy Efficient Ethernet**—Check **Enable** to enable Energy Efficient Ethernet on the port, or uncheck to disable it on the port.

STEP 3 Click **Apply**. The Energy Efficient Ethernet is enabled or disabled on the port, and the Running Configuration is updated.

10

Power over Ethernet

The Power over Ethernet (PoE) feature is only available on PoE-based models. For a list of PoE-based models, refer to the **Device Models** section.

This chapter describes how to use the PoE feature and includes the following topics:

- **PoE Considerations**
- **PoE on the Switch**
- **Configuring PoE Properties**
- **Configuring PoE Port Settings**

PoE Considerations

Model	Power Dedicated to PoE	PoE Ports	PoE Standard Supported
SF220-24P	180 Watts	1 to 24	802.3at
SF220-26P	180 Watts	1 to 24	802.3at
SF220-48P	375 Watts	1 to 48	802.3at
SG220-50P	375 Watts	1 to 48	802.3at
SF220-28MP	375 Watts	1 to 24	802.3at

CAUTION The switch should be connected only to PoE networks without routing to the outside plant.

CAUTION Consider the following when connecting switches capable of supplying PoE:

The PoE models of the switches are Power Sourcing Equipments (PSEs) that are capable of supplying DC power to attaching Powered Devices (PDs). These devices include VoIP phones, IP cameras, and wireless access points. The PoE switches can detect and supply power to pre-standard legacy PoE Powered Devices. Due to the support of legacy PoE, 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 PSEs, 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.

PoE on the Switch

A PoE switch is Power Sourcing Equipment (PSE) that delivers electrical power to the connected powered devices (PD) over existing copper cables without interfering with the network traffic, updating the physical network or modifying the network infrastructure.

PoE Features

PoE provides the following features:

- Eliminates the need to run 110/220 V AC power to all devices on a wired LAN.
- Removes the necessity for placing all network devices next to power sources.
- Eliminates the need to deploy double cabling systems in an enterprise significantly decreasing installation costs.

PoE can be used in any enterprise network that deploys relatively low-powered devices connected to the Ethernet LAN, such as:

- IP phones
- Wireless access points
- IP gateways
- Audio and video remote monitoring devices

PoE Operation

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 PSE and the PD commences after the Detection stage. During negotiation, the PD specifies its class, which is the amount of maximum power that the PD consumes.
- **Power Consumption**—After the classification stage completes, the PSE provides power to the powered device (PD). The PD without classification support will be 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 that the switch agrees to supply is limited to the value that the system administrator configures, regardless of the classification result.
- **Class Limit**—The maximum power that the switch agrees to supply is determined by the results of the classification stage. This means that it is set as per the client's request.

PoE Configuration Considerations

There are two factors to consider in the PoE feature:

- The amount of power that the PSE can supply
- The amount of power that the PD is actually attempting to consume

You can decide the following:

- During device operation, to change the mode from Class Limit to Port Limit and vice versa. The power values per port that were configured for the Port Limit mode are retained.

  NOTE Changing the mode from Class Limit to Port Limit and vice versa when the switch is operational forces the PD to be reconnected.

- Maximum port limit allowed as a per-port numerical limit in mW (Port Limit mode).
- To generate a trap when a PD tries to consume too much and at what percent of the maximum power this trap is generated.

In the Class Limit mode, the PoE-specific hardware automatically detects the PD class and its power limit according to the class of the device connected to each specific port.

If at any time during the connectivity an attached PD requires more power from the switch than the configured allocation allows (no matter if the switch is in Class Limit or Port Limit mode), the switch does the following:

- Maintains the up/down status of the PoE port link
- Turns off power delivery to the PoE port
- Maintains the power delivery to other PoE ports
- Logs the reason for turning off power
- Generates an SNMP trap

Configuring PoE Properties

Use the Properties page to select PoE operation mode (Port Limit or Class Limit), and specify 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.

Power is disabled during power-on reboot, initialization, and system configuration to ensure that PDs are not damaged.

To configure PoE and monitor current power usage:

STEP 1 Click **Port Management** > **PoE** > **PoE Properties**.

STEP 2 Enter the following information:

- **Power Mode**—Select one of the following options:
  - *Port Limit*—The maximum power limit per each port is configured by the user.
  - *Class Limit*—The maximum power limit per port is determined by the class of the device, which results from the classification stage.

  NOTE When you change from Port Limit to Class Limit or vice versa, the ports will be reconnected.
- **Legacy**—Enables or disables supporting legacy powered devices. This feature only works when establishing the connection auto-negotiation. For the legacy powered devices that are already connected, disabling this feature only takes effect after you unplug their cables.
- **Traps**—Enables or disables traps. If traps are enabled, you must also enable the SNMP service and configure at least one SNMP notification recipient (see **Configuring SNMP Notification Recipients**).
- **Power Trap Threshold**—Enters the usage threshold that is a percentage of the system power. An alarm is initiated if the power exceeds this value.

The following counters are displayed for each device:

- **Operational Status**—Displays the operational status (Normal or Fault) of the PoE switch.
- **Nominal Power**—Displays the total amount of power that the switch can supply to all connected PDs.
- **Consumed Power**—Displays the amount of power currently being consumed by the PoE ports.
- **Allocated Power**—Displays the amount of power allocated for the PoE ports.
- **Available Power**—Nominal power minus the amount of allocated power.

STEP 3 Click **Apply**. The PoE properties are defined, and the Running Configuration is updated.

Configuring PoE Port Settings

Use the PoE Port Settings page to enable PoE on the ports and monitor the current power usage and maximum power limit per port.

This page limits the power per port in two ways depending on the power mode:

- **Port Limit**—Power is limited to a specified wattage. For these settings to be active, the switch must be in Port Limit mode. That mode is configured on the PoE Properties page. When the power consumed on the port exceeds the port limit, the port power is turned off.
- **Class Limit**—Power is limited based on the class of the connected PD. For these settings to be active, the switch must be in Class Limit mode. That mode is configured on the PoE Properties page. When the power consumed on the port exceeds the class limit, the port power is turned off.

To configure PoE port settings:

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

STEP 2 To edit the power limit per port, select a port and click **Edit.**

STEP 3 Enter the following information:

- **Interface**—Select the port to be configured.
- **PoE Administrative Status**—Enable or disable PoE on the port.
- **Time Range**—Select to enabled PoE on the port.
- **Time Range Name**—If Time Range has been enabled, select the time range to be used. Time ranges are defined in the Time Range page.
- **Power Priority Level**—Select the port priority for power management when the switch power supply is insufficient. For example, when the system power is not sufficient, and the PD is inserted into port 1, which is prioritized as high, the power to ports with low priority may be cut off.
- **Administrative Power Allocation**—If the power mode is Power Limit, enter the maximum amount of power in milliwatts allocated to the port. The default is 30,000 mW.

The following counters are displayed for each device:

- **Max Power Allocation**—Displays the maximum amount of power in milliwatts assigned to the PD connected to the selected port. In Class Limit mode, the value of the maximum power allocation will be determined on the class detection of PD connected, 15.4 w (802.3af, class 0 to 3), and 30 W (802.3at, class 4). In Power Limit mode, the value of maximum power allocation is 30 W.
- **Power Consumption**—Displays the amount of power in milliwatts assigned to the powered device connected to the selected port.
- **Class**—Displays the class information of the PD connected if the power mode is Class Limit.

Class	Maximum Power Delivered by Switch Port
Class 0	15.4 W
Class 1	4.0 W
Class 2	7.0 W
Class 3	15.4 W
Class 4	30.0 W

- **Overload Counter**—Displays the total number of power overload occurrences.
- **Short Counter**—Displays the total number of power shortage occurrences.
- **Denied Counter**—Displays the number of times that the powered device was denied power.
- **Absent Counter**—Displays the number of times that the power was stopped to the powered device because the powered device was no longer detected.
- **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 port settings are defined, and the Running Configuration is updated.

11

Managing VLANs

This chapter describes how to configure the VLAN settings and includes the following topics:

- VLANs
- Configuring Default VLAN
- Creating VLANs
- Configuring Interface's VLAN Settings
- Configuring Port to VLAN
- Viewing VLAN Membership
- Configuring GVRP
- Configuring Voice VLAN

VLANs

A VLAN is a logical group of ports that enables devices associated with it to communicate with each other over the Ethernet MAC layer, regardless of the physical LAN segment of the bridged network to which they are connected.

VLAN Description

Each VLAN is configured with a unique VID (VLAN ID) with a value from 1 to 4094. A port on a device in a bridged network is a member of a VLAN if it can send data to and receive data from the VLAN. A port is an untagged member of a VLAN if all packets destined for that port into the VLAN have no VLAN tag. A port is a tagged member of a VLAN if all packets destined for that port into the VLAN have a VLAN tag. A port can be a member of one or more VLANs.

A port in VLAN Access mode can be part of only one VLAN. If it is in General or Trunk mode, the port can be part of one or more VLANs.

VLANs address security and scalability issues. Traffic from a VLAN stays within the VLAN, and terminates at devices in the VLAN. It also eases network configuration by logically connecting devices without physically relocating those devices.

If a frame is VLAN-tagged, a four-byte VLAN tag is added to each Ethernet frame. The tag contains a VLAN ID between 1 and 4094, and a VLAN Priority Tag (VPT) between 0 and 7.

When a frame enters a VLAN-aware device, it is classified as belonging to a VLAN, based on the four-byte VLAN tag in the frame.

If there is no VLAN tag in the frame or the frame is priority-tagged only, the frame is classified to the VLAN based on the Port VLAN Identifier (PVID) configured at the ingress port where the frame is received.

The frame is discarded at the ingress port if Ingress Filtering is enabled and the ingress port is not a member of the VLAN to which the packet belongs. A frame is regarded as priority-tagged only if the VID in its VLAN tag is 0.

Frames belonging to a VLAN remain within the VLAN. This is achieved by sending or forwarding a frame only to egress ports that are members of the target VLAN. An egress port may be a tagged or untagged member of a VLAN.

The egress port:

- Adds a VLAN tag to the frame if the egress port is a tagged member of the target VLAN, and the original frame does not have a VLAN tag.
- Removes the VLAN tag from the frame if the egress port is an untagged member of the target VLAN, and the original frame has a VLAN tag.

VLAN Roles

VLANs function at Layer 2. All VLAN traffic (Unicast, Broadcast, and Multicast) remains within its VLAN. Devices attached to different VLANs do not have direct connectivity to each other over the Ethernet MAC layer.

Adjacent VLAN-aware devices exchange VLAN information with each other by using Generic VLAN Registration Protocol (GVRP). As a result, VLAN information is propagated through a bridged network. VLANs on a device can be created statically or dynamically, based on the GVRP information exchanged by devices. A VLAN can be static or dynamic (from GVRP), but not both. For more information about GVRP, refer to the **Configuring GVRP** section.

Some VLANs can have additional roles, including:

- **Voice VLAN**—Refer to the **Configuring Voice VLAN** section for more information.
- **Guest VLAN**—Set up on the Edit VLAN Authentication page.
- **Default VLAN**—Refer to the **Configuring Default VLAN** section for more information.
- **Management VLAN** (in Layer 2-system-mode systems)—Refer to the **IP Addressing** section for more information.

Workflow to Configure VLANs

To configure VLANs:

- If required, change the default VLAN as described in the **Configuring Default VLAN** section.
- Create the required VLANs as described in the **Creating VLANs** section.
- Set the desired per port VLAN-related configuration as described in the **Configuring Interface's VLAN Settings** section.
- Assign interfaces to VLANs as described in the **Configuring Port to VLAN** section.
- View the current VLAN port membership for all interfaces as described in the **Viewing VLAN Membership** section.
- Enable GVRP globally as well as on each port as described in the **Configuring GVRP** section.
- Configure the voice VLAN parameters as described in the **Configuring Voice VLAN** section.

Configuring Default VLAN

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 ports are configured as untagged members of the default VLAN.

The default VLAN has the following characteristics:

- Distinct, nonstatic, 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:

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.

Creating VLANs

You can create a VLAN, but this has no effect until the VLAN is attached to at least one port, either manually or dynamically. Ports must always belong to one or more VLANs.

Each VLAN must be configured with a unique VID (VLAN ID) with a value from 1 to 4094. The switch reserves VID 4095 as the Discard VLAN. All packets classified to the Discard VLAN are discarded at ingress, and are never forwarded to a port.

To create a VLAN:

STEP 1 Click **VLAN Management** > **Create VLAN**.

The following fields are displayed:

- **VLAN ID**—Identifier of the VLAN.
- **VLAN Name**—Name of the VLAN.
- **Type**—The type of VLAN. The options are:
  - *GVRP*—The VLAN was dynamically created through Generic VLAN Registration Protocol (GVRP).
  - *Static*—The VLAN is user-defined.
  - *Default*—The VLAN is the default VLAN.

STEP 2 Click **Add** to add a new VLAN or select an existing VLAN and click **Edit** to modify the VLAN parameters.

STEP 3 To create a single VLAN, select the **VLAN** radio button, enter the **VLAN ID (VID)**, and optionally the **VLAN Name**.

STEP 4 To create a range of VLANs, select the **Range** radio button, and specify the range of VLANs to be created in the **VLAN Range** fields.

STEP 5 Click **Apply**. The VLANs are created, and the Running Configuration is updated.

Configuring Interface's VLAN Settings

Use the Interface Settings page to configure the VLAN-related parameters for all interfaces. The switch supports 4094 VLANs, including the default VLAN.

To configure the interface's VLAN settings:

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

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

STEP 3 Select a port or LAG, and click **Edit**.

STEP 4 Enter the following information:

- **Interface**—Select a port or a LAG to configured.
- **Interface VLAN Mode**—Select the VLAN mode. The options are:
  - *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.
  - *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.
  - *Dot1p-Tunnel*—Selecting this option places the interface in QinQ mode. This enables the user to use their own VLAN arrangements (PVID) across the provider network. The switch will be in QinQ mode when it has one or more dot1p-tunnel ports.
- **Administrative PVID**—(Available in General and Trunk modes) Enter the Port VLAN ID (PVID) of the VLAN to which incoming untagged and priority tagged frames are classified.
- **Frame Type**—(Available in General mode) Select the type of frame that the interface can receive. Frames that are not of the configured frame type are discarded at ingress. These frame types are only available in General mode. 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 in General mode) Check **Enable** 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 is not a member. Ingress filtering can be disabled or enabled on general ports. It is always enabled on access ports and trunk ports.
- **Uplink**—(Available in Trunk mode) Check **Enable** to set the interface as an uplink port.

- **TPID**—(Available in Trunk mode) If Unlink is enabled, select the Modified Tag Protocol Identifier (TPID) value for the interface.

STEP 5 Click **Apply**. The interface's VLAN settings are defined, and the Running Configuration is updated.

Configuring Port to VLAN

Use the Port to VLAN page to configure the port members of a VLAN.

To map ports or LAGs to a VLAN:

STEP 1 Click **VLAN Management** > **Port to VLAN**.

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

The port mode for each port or LAG is displayed with its current port mode (Access, Trunk, General, or Dot1q-Tunnel) configured on the Interface Settings page.

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

- **Forbidden**—The interface is not allowed to join the VLAN even from GVRP registration. When a port is not 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. The port can join the VLAN through GVRP registration.
- **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 the Running Configuration is updated.

Viewing VLAN Membership

The Port VLAN Membership page displays a list of VLANs to which each port belongs.

When a port is forbidden default VLAN membership, that port is not allowed membership in any other VLAN. An internal VID of 4095 is assigned to the port.

To forward the packets properly, intermediate VLAN-aware devices that carry VLAN traffic along the path between end nodes must either be manually configured or must dynamically learn the VLANs and their port memberships from GVRP.

Untagged port membership between two VLAN-aware devices with no intervening VLAN-aware devices, should be to the same VLAN. In other words, the PVID on the ports between the two devices must be the same if the ports are to send and receive untagged packets to and from the VLAN. Otherwise, traffic might leak from one VLAN to another.

Frames that are VLAN-tagged can pass through other network devices that are VLAN-aware or VLAN-unaware. If a destination end node is VLAN-unaware, but is to receive traffic from a VLAN, then the last VLAN-aware device (if there is one), must send frames of the destination VLAN to the end node untagged.

To view VLAN membership:

STEP 1 Click **VLAN Management** > **Port VLAN Membership**.

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

The following fields are displayed:

- **Interface**—Port or LAG ID.
- **Mode**—Interface VLAN mode that was selected on the Interface Settings page.
- **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 the interface selected is Port, displays the LAG in which it is a member.

STEP 3 Select a port, and click **Join VLAN**.

STEP 4 Enter the following information:

- **Interface**—Select the port or LAG to be defined.
- **Mode**—Displays the port VLAN mode that was selected on the Interface Settings page.
- **Select VLAN**—To associate a port with the VLANs, move the VLAN IDs from the left list to the right list by using the arrow buttons. The default VLAN might appear in the right list if it is tagged, but it cannot be selected.
- **Tagging**—Select one of the following tagging or PVID options:
  - *Forbidden*—The interface is not allowed to join the VLAN even from GVRP registration. When a port is not 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. The port can join the VLAN through GVRP registration.
  - *Tagged*—Select whether the port is tagged. This is not relevant for Access ports.
  - *Untagged*—Select whether port is untagged. This is not relevant for Access ports.
  - *PVID*—Port PVID is set to this VLAN. If the interface is in access mode or trunk mode, the switch automatically makes the interface an untagged member of the VLAN. If the interface is in General mode, you must manually configure VLAN membership.

STEP 5 Click **Apply**. The settings are modified, and the Running Configuration is updated.

STEP 6 To see the administrative and operational VLANs on an interface, click **Details**.

Configuring GVRP

Adjacent VLAN-aware devices can exchange VLAN information with each other by using Generic VLAN Registration Protocol (GVRP). GVRP is based on the Generic Attribute Registration Protocol (GARP) and propagates VLAN information throughout a bridged network.

Since GVRP requires support for tagging and should trunk allowed VLAN, so the port must be configured in Trunk mode.

When a port joins a VLAN by using GVRP, it is added to the VLAN as a dynamic member, unless this was expressly forbidden on the Port VLAN Membership page. If the VLAN does not exist, it is dynamically created when Dynamic VLAN creation is enabled for this port (on the GVRP Settings page).

GVRP must be activated globally as well as on each port. When it is activated, it transmits and receives GARP Packet Data Units (GPDUs). VLANs that are defined but not active are not propagated. To propagate the VLAN, it must be up on at least one port.

To define the GVRP settings:

STEP 1 Click **VLAN Management** > **GVRP Settings**.

STEP 2 Check **Enable** next to the **GVRP Global Status** field to globally enable GVRP on the switch.

STEP 3 Click **Apply**.

STEP 4 Select the interface type (Port or LAG), and click **Go**.

The following fields are displayed:

- **Interface**—Interface number.
- **GVRP State**—Displays whether GVRP is enabled or disabled on the interface.
- **Dynamic VLAN Creation**—Displays whether Dynamic VLAN creation is enabled or disabled on the interface. If it is disabled, GVRP can operate but new VLANs are not created.
- **GVRP Registration**—Displays the VLAN registration mode on the interface.

STEP 5 To define the GVRP settings for an interface, select the desired interface and click **Edit**.

STEP 6 Enter the following information:

- **Interface**—Select the port or LAG to be defined.
- **GVRP State**—Check **Enable** to enable GVRP on this interface.
- **Dynamic VLAN Creation**—Check **Enable** to enable Dynamic VLAN Creation on this interface.
- **GVRP Registration**—Select the VLAN Registration mode using GVRP on this interface.

STEP 7 Click **Apply**. The GVRP settings are modified, and the Running Configuration is updated.

Configuring Voice VLAN

In a LAN, voice devices, such as IP phones, VoIP endpoints, and voice systems are placed into the same VLAN. This VLAN is referred as the voice VLAN. The voice VLAN is used when traffic from VoIP equipment or phones is assigned to a specific VLAN. The switch can automatically detect and add port members to the voice VLAN, and assign the configured quality of service (QoS) to packets from the voice VLAN.

Dynamic Voice VLAN Modes

The switch supports two dynamic voice VLAN modes. They are Telephony OUI (Organization Unique Identifier) mode and Auto Voice VLAN mode. The two modes affect how voice VLAN and/or voice VLAN port memberships are configured. The two modes are mutually exclusive to each other.

- **Telephony OUI**—In Telephony OUI mode, the voice VLAN must be a manually configured VLAN, and cannot be the default VLAN.

  When the switch is in Telephony OUI mode and a port is manually configured as a candidate to join the voice VLAN, the switch dynamically adds the port to the voice VLAN if it receives a packet with a source MAC address matching to one of the configured telephony OUIs. An OUI is the first three bytes of an Ethernet MAC address. For more information about Telephony OUI, see the **Configuring Telephony OUI** section.

- **Auto Voice VLAN**—In Auto Voice VLAN mode, the voice VLAN can be either the default voice VLAN or manually configured.

Unlike Telephony OUI mode that detects voice devices based on telephony OUI, Auto Voice VLAN mode dynamically adds the ports to the voice VLAN depending on CDP and/or LLDP MED, if enabled. Add a port to the voice VLAN if it detects an attaching device to the port that advertises itself as a phone or media end points through CDP and/or LLDP MED.

Voice VLAN Constraints

The following constraints exist:

- Only one voice VLAN is supported.
- A VLAN that is defined as a voice VLAN cannot be removed.

In addition, the following constraints are applicable for Telephony OUI:

- The voice VLAN cannot be VLAN1 (the default VLAN).
- A new VLAN ID can be configured for the voice VLAN only if the current voice VLAN does not have candidate ports.
- The voice VLAN cannot be the Guest VLAN if the voice VLAN mode is set to Telephony OUI.
- The interface VLAN of a candidate port must be in General mode or Trunk mode.
- The voice VLAN QoS decision has priority over any other QoS decision, except for the Policy/ACL QoS decision.
- The voice VLAN QoS is applied to candidate ports that have joined the voice VLAN, and to static ports.

Voice VLAN Options

You can perform the following operations with this feature:

- Set the global voice VLAN settings and the mode of dynamic voice VLAN as described in the **Configuring Voice VLAN Properties** section.
- Configure and update the Telephony OUI table with up to 16 entries (each entry is a three-octet number) as described in the **Configuring Telephony OUI** section. The switch uses the table to determine if a port has Auto Voice VLAN Membership enabled and will join the voice VLAN.
- Add an interface to the voice VLAN on the basis of the OUI identifier and to configure the OUI QoS mode of voice VLAN as described in the **Adding Interfaces to Voice VLAN on Basis of OUIs** section.

Configuring Voice VLAN Properties

Use the Properties page to globally configure the voice VLAN parameters.

To configure the voice VLAN properties:

STEP 1 Click **VLAN Management** > **Voice VLAN** > **Properties**.

STEP 2 Enter the following information:

- **Voice VLAN ID**—Select the VLAN as the voice VLAN.
- **CoS/802.1p**—Select the CoS/802.1p value that will be used by LLDP MED as a voice network policy. The possible values are 0 to 7, where 7 is the highest priority. 0 is used as a best effort, and is invoked automatically when no other value has been set (default).
- **DSCP**—Select the DSCP value that will be used by LLDP MED as a voice network policy.
- **Dynamic Voice VLAN**—Select one of the following voice VLAN modes:
  - *Enable Auto Voice VLAN*—Select this option to enable the Auto Voice VLAN mode.
  - *Enable Telephony OUI*—Select this option to enable the Telephony OUI mode.
  - *Disable*—Select this option to disable the Voice VLAN.

STEP 3 Click **Apply**. The VLAN properties are defined, and the Running Configuration is updated.

Configuring 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.

The OUI Global table can hold up to 16 OUIs.

Use the Telephony OUI page to configure the Telephony OUI settings. If the specified Auto Membership Aging Time passes with no telephony activity, the port is removed from the voice VLAN.

To configure Telephony OUI:

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

The Telephony OUI table displays the following information:

- **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**—Check to remark egress traffic.
- **Auto Membership Aging Time**—Enter the time delay to remove a port from the voice VLAN after all MAC addresses of the phones detected on the ports have aged out.

STEP 3 Click **Apply**.

STEP 4 Click **Add** to add an OUI.

STEP 5 Enter the following information:

- **Telephony OUI**—Enter a new OUI.
- **Description**—Enter an OUI name.

STEP 6 Click **Apply**. The OUI is added, and the Running Configuration is updated.

STEP 7 Click **Restore Default OUI** to delete all user-created OUIs, and leave only the default OUIs in the table.

Adding Interfaces to Voice VLAN on Basis of OUIs

The QoS attributes can be assigned per port to the voice packets in one of the following modes:

- **All**—The QoS values configured to the voice VLAN are applied to all 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 ID and to configure the OUI QoS mode of the voice VLAN.

To configure Telephony OUI on an interface:

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

STEP 2 To configure an interface to be a candidate port of the telephony OUI-based voice VLAN, select the desired interface and click **Edit**.

STEP 3 Enter the following information:

- **Interface**—Select the port or LAG to be configured.
- **Telephone OUI VLAN Membership**—Check **Enable** to set the interface as a candidate port of the telephony OUI-based voice VLAN. When packets that match one of the configured telephony OUI are received, the interface is added to the voice VLAN.
- **Telephone OUI Mode**—Select either **Auto** or **Manual** as the port mode.
  - *Auto*—The port is identified as a candidate to join the Voice VLAN. When a packet with a source OUI MAC address that identifies the remote equipment as voice equipment is seen on the port, the port joins the voice VLAN as a tagged port. If the time since the last telephony MAC address was aged out of the MAC address table exceeds the voice VLAN aging time, the port is removed from the voice VLAN.
  - *Manual*—Manually assigned to the voice VLAN.
- **Telephony OUI QoS Mode**—Select one of the following options:
  - *Telephony Source MAC Address*—QoS attributes are applied only on packets from IP phones.

- *All*—QoS attributes are applied only on all packets that are classified to the voice VLAN.

STEP 4 Click **Apply**. The Telephony OUI interface settings are defined, and the Running Configuration is updated.

12

Spanning Tree Protocol

The Spanning Tree Protocol (STP) (IEEE802.1D and IEEE802.1Q) is enabled by default, set to Classic STP mode.

This chapter describes how to configure STP and contains the following topics:

- **STP Modes**
- **Configuring STP Status and Global Settings**
- **Configuring STP Interface Settings**
- **Configuring RSTP Interface Settings**
- **Configuring Multiple Spanning Tree**

STP Modes

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.

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause switches to forward traffic indefinitely, resulting in increased traffic and reduced network efficiency.

STP provides a tree topology for any arrangement of switches and interconnecting links, creating a unique path between end stations on a network, eliminating loops.

The switch supports the following STP modes:

- **Classic STP**—Provides a single path between any two end stations, avoiding and eliminating loops.
- **Rapid STP (RSTP)**—Detects network topologies to provide faster convergence of the spanning tree. This is most effective when the network topology is naturally tree-structured, and therefore faster convergence might be possible. RSTP is enabled by default.
- **Multiple STP (MSTP)**—MSTP is based on RSTP. It detects Layer 2 loops, and attempts to mitigate them by preventing the involved port from transmitting traffic. Since loops exist on a per-Layer 2-domain basis, a situation can occur where there is a loop in VLAN A and no loop in VLAN B. If both VLANs are on Port X, and STP wants to mitigate the loop, it stops traffic on the entire port, including VLAN B traffic.

  MSTP solves this problem by enabling several STP instances, so that it is possible to detect and mitigate loops separately in each instance. By associating instances to VLANs, each instance is associated with the Layer 2 domain on which it performs loop detection and mitigation. This enables a port to be stopped in one instance, such as traffic from VLAN A that is causing a loop, while traffic can remain active in another domain where no loop was seen, such as on VLAN B.

Configuring STP Status and Global Settings

Use the STP Status and Global Settings page to enable STP, RSTP, or MSTP on the switch.

Use the STP Interface Settings page, RSTP Interface Settings page, and MSTP Properties page to configure each mode, respectively.

To set STP status and global settings:

STEP 1 Click **Spanning Tree** > **STP Status and Global Settings**.

STEP 2 In the **Global Settings** area, enter the following information:

- **Spanning Tree State**—Enable or disable STP on the switch.
- **STP Loopback Guard**—Select to enable Loopback Guard on the device.
- **STP Operation Mode**—Select the STP mode.

- **BPDU Handling**—Select how Bridge Protocol Data Unit (BPDU) packets are managed when STP is disabled on the switch. BPDUs are used to transmit spanning tree information. The options are:
  - *Filtering*—Filters BPDU packets when STP is disabled.
  - *Flooding*—Floods BPDU packets when STP is disabled.
- **Path Cost Default Values**—Select the method used to assign default path costs to the STP ports. The default path cost assigned to a port varies according to the selected method.
  - *Short*—Specifies the range 1 through 65,535 for port path costs.
  - *Long*—Specifies the range 1 through 200,000,000 for port path costs.

STEP 3 In the **Bridge Settings** area, enter the following information:

- **Priority**—Enter the bridge priority value. After exchanging BPDUs, the device with the lowest priority becomes the Root Bridge. In the situation when all bridges use the same priority, then their MAC addresses are used to determine which is the Root Bridge. The bridge priority value is provided in increments of 4096. For example, 4096, 8192, 12288, and so on.
- **Hello Time**—Enter the interval in seconds that a Root Bridge waits between configuration messages. The range is 1 to 10 seconds. The default is 2 seconds.
- **Max Age**—Enter the interval in seconds that the switch can wait without receiving a configuration message, before attempting to redefine its own configuration. The range is 6 to 40 seconds. The default is 20 seconds.
- **Forward Time**—Enter the interval in seconds that a bridge remains in a learning state before forwarding packets. The range is 4 to 30 seconds. The default is 15 seconds.

In the **Designated Root** area, the following fields are displayed:

- **Bridge ID**—The bridge priority concatenated with the MAC address of the switch.
- **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. (This is significant when the bridge is not the root.)
- **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 is displayed in a days/hours/minutes/seconds format.

STEP 4 Click **Apply**. The STP global settings are defined, and the Running Configuration is updated.

Configuring STP Interface Settings

Use the STP Interface Settings page to configure STP per interface, and to view information learned by the protocol, such as the designated bridge.

The configuration entered on this page is active for all STP modes.

To configure STP on an interface:

STEP 1 Click **Spanning Tree** > **STP 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 the port or LAG to be defined.
- **Edge Port**—Enable or disable Fast Link on the interface. If Fast Link mode is enabled for an interface, the interface state is automatically placed in the Forwarding state when the interface link is up. Fast Link optimizes the STP protocol convergence.
- **BPDU Guard**—If enabled, the interface will shut down when a BPDU message is received.
- **BPDU Filter**—If enabled, the interface will not send and receive BPDU messages.
- **Path Cost**—Select **User Defined** to enter the port contribution to the root path cost, or select **Use Default** to use the default cost generated by the system.

- **Priority**—Select the priority value of the interface. The priority value influences the interface choice when a bridge has two ports connected in a loop. The priority is a value from 0 to 240, set in increments of 16.
- **Port State**—Displays the current STP state of the interface.
  - *Disabled*—STP is currently disabled on the interface. The interface forwards traffic while learning MAC addresses.
  - *Blocking*—The interface is currently blocked, and cannot forward traffic (with the exception of BPDU data) or learn MAC addresses.
  - *Learning*—The interface is in Learning mode, and cannot forward traffic, but it can learn new MAC addresses.
  - *Forwarding*—The interface is in Forwarding mode, and 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 ID of the selected interface.
- **Designated Cost**—Displays the cost of the interface participating in the STP topology. Interfaces with a lower cost are less likely to be blocked if STP detects loops.

STEP 5 Click **Apply**. The STP interface settings are modified, and the Running Configuration is updated.

Configuring RSTP Interface Settings

Rapid Spanning Tree Protocol (RSTP) enables a faster STP convergence without creating forwarding loops.

Use the RSTP Interface Settings page to configure RSTP per port. Any configuration that is done on this page is active when the global STP mode is set to RSTP or MSTP.

To define the RSTP interface settings:

STEP 1 Set the STP operation mode to RSTP as described in the **Configuring STP Status and Global Settings** section.

STEP 2 Click **Spanning Tree** > **RSTP Interface Settings**.

STEP 3 Select the interface type (Port or LAG) and click **Go**.

STEP 4 Select an interface and click **Edit**.

STEP 5 Enter the following information:

- **Interface**—Set the port or LAG to be configured.
- **Point-to-Point Administrative Status**—Define the link status. The available options are:
  - *Enable*—The port link type is **point-to-point**.
  - *Disable*—The port link type is **share**.
  - *Auto*—Automatically determines the port link type status by using the port link up duplex mode (**point-to-point** for full duplex mode and **share** for half duplex mode).
- **Point-to-Point Operational Status**—Displays the current link-type operating status.
- **Role**—Displays the role of the interface that has been assigned by STP to provide STP paths. The possible roles are:
  - *Root*—Lowest cost path to forward packets to the Root Bridge.
  - *Designated*—The port through which the bridge is connected to the LAN that provides the lowest cost path from the LAN to the Root Bridge.
  - *Alternate*—Provides an alternate path to the Root Bridge from the root interface.
  - *Backup*—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 connections connected 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 or disabled on the interface.
- **Port Status**—Displays the RSTP status of the interface. The values are:
  - *Disabled*—RSTP is currently disabled on the interface.
  - *Blocking*—The interface is currently blocked, and cannot forward traffic or learn MAC addresses.
  - *Learning*—The interface is in learning mode, and cannot forward traffic, however it can learn new MAC addresses.
  - *Forwarding*—The interface is in Forwarding mode, and can forward traffic and learn new MAC addresses.

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

STEP 7 If the selected interface connects to the bridge partner being tested, the Activate Protocol Migration is activated. When a link partner is discovered by using STP, click **Activate Protocol Migration** to run a Protocol Migration test. This test 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.

Configuring Multiple Spanning Tree

Multiple Spanning Tree Protocol (MSTP) is used to separate the STP port state between various domains (on different VLANs). For example, while port A is blocked in one STP instance due to a loop on VLAN A, the same port can be placed in the Forwarding State in another STP instance.

To configure MSTP:

STEP 1 Set the STP operation mode to MSTP as described in the **Configuring STP Status and Global Settings** section.

STEP 2 Define global MSTP parameters as described in the **Configuring MSTP Properties** section.

STEP 3 Define MSTP instances as described in the **Configuring MSTP Instance Settings** section. Each MSTP instance calculates and builds a loop-free topology to bridge packets from the VLANs that map to the instance.

STEP 4 Decide which MSTP instance is active in what VLAN, and associate these MSTP instances to VLANs accordingly as described in the **Mapping VLANs to MST Instance** section.

Configuring MSTP Properties

Use the MSTP Properties page to define the global MSTP settings. 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. MSTP allows formation of MSTP regions that can run multiple MST Instances (MSTIs). 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. MSTP not only allows 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 MSTP region, they must have the same VLANs-to-MSTP instance mapping, the same configuration revision number, and the same region name. This mapping can be done on the VLAN to MSTP Instance page.

Switches intended to be in the same MSTP region are never separated by switches from another MSTP region. If they are separated, the region becomes two separate regions.

To define global MSTP properties:

STEP 1 Click **Spanning Tree** > **MSTP Properties**.

STEP 2 Enter the following information:

- **Region Name**—Enter the MSTP region name.
- **Revision**—Enter an unsigned 16-bit number that identifies the revision of the current MSTP configuration. The field range is from 0 to 65535.

- **Max Hops**—Enter 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 from 1 to 40. The default is 20.

STEP 3 Click **Apply**. The MSTP properties are defined, and the Running Configuration file is updated.

Mapping VLANs to MST Instance

Use the VLAN to MSTP Instance page to map VLANs to MSTP instances. For devices to be in the same region, they must have the same VLAN to MSTP instance mappings.

NOTE The same MSTP instance can be mapped with more than one VLAN, but each VLAN can only have one MSTP instance attached to it.

Up to 16 MSTP instances can be defined on the switch. For those VLANs that are not explicitly mapped to one of the MSTP instances, the switch automatically maps them to the Core and Internal Spanning Tree (CIST) instance. The CIST instance is MSTP instance 0.

To map VLANs to MSTP instances:

STEP 1 Click **Spanning Tree** > **VLAN to MSTP Instance**.

STEP 2 To add VLANs to an MSTP instance, select the desired MSTP instance and click **Edit**.

STEP 3 Enter the following information:

- **MSTP Instance ID**—Select the MSTP instance.
- **VLANs**—Enter the VLANs being mapped to this MSTP instance.
- **Action**—Select either **Add** or **Remove** to map or remove the VLANs to or from the MSTP instance.

STEP 4 Click **Apply**. The VLAN-to-MSTP instance mapping is defined, and the Running Configuration file is updated.

Configuring MSTP Instance Settings

Use the MSTP Instance Settings page to configure the MSTP instance settings.

To define the settings for an MSTP instance:

STEP 1 Click **Spanning Tree** > **MSTP Instance Settings**.

STEP 2 Enter the following information:

- **Instance ID**—Select the MSTP instance to be configured.
- **Included VLAN**—Displays the VLANs mapped to the selected MSTP instance. The default mapping is that all VLANs are mapped to the CIST instance (instance 0).
- **Priority**—Enter the priority of this bridge for the selected MSTP instance.
- **Designated Root Bridge ID**—Displays the priority and MAC address of the Root Bridge for the selected MSTP instance.
- **Root Port**—Displays the root port of the selected MSTP instance.
- **Root Path Cost**—Displays the root path cost of the selected MSTP instance.
- **Bridge ID**—Displays the bridge priority and the MAC address of this switch for the selected MSTP instance.
- **Remaining Hops**—Displays the number of hops remaining to the next destination.

STEP 3 Click **Apply**. The MSTP instance settings are modified, and the Running Configuration is updated.

Configuring MSTP Interface Settings

Use the MSTP Interface Settings page to configure the MSTP interface settings for each MSTP instance, and to view information that has currently been learned by the protocol, such as the designated bridge per MSTP instance.

To configure the MSTP interface settings:

STEP 1 Click **Spanning Tree** > **MSTP Interface Settings**.

STEP 2 Select an MSTP instance and the interface type (Port or LAG) and click **Go**.

The MSTP settings for the interfaces on the instance are displayed.

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

STEP 4 Enter the following information:

- **Instance ID**—Select the MSTP instance to be configured.
- **Interface**—Select the port or LAG to be configured.
- **Path Cost**—Select **User Defined** to set the port contribution to the root path cost, or select **Use Default** to use the default value. The root path cost is the cost of the switch to the Root Bridge of the specified MSTP instance.
- **Priority**—Enter the port priority for the selected port and MSTP instance.
- **Port State**—Displays the MSTP status of the port. The values are:
  - *Disabled*—MSTP is currently disabled.
  - *Blocking*—The port on this instance is currently blocked, and cannot forward traffic (with the exception of BPDU data) or learn MAC addresses.
  - *Learning*—The port on this instance is in Learning mode, and cannot forward traffic. But it can learn new MAC addresses.
  - *Forwarding*—The port on this instance is in Forwarding mode, and can forward traffic and learn new MAC addresses.
- **Port Role**—Displays the port role 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 port provides the lowest cost path to forward packets to the root device.
  - *Designated*—The port through which the bridge is connected to the LAN that provides the lowest root path cost from the LAN to the Root Bridge for the MST instance.
  - *Alternate*—The port provides an alternate path to the root device from the root interface.

  - *Backup*—The port 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 connections connected to a shared segment.
  - *Disabled*—The port does not participate in the Spanning Tree.
- **Mode**—Displays the current Spanning Tree mode.
  - *STP*—Classic STP is enabled on the port.
  - *Rapid STP*—RSTP is enabled on the port.
  - *MSTP*—MSTP is enabled on the port.
- **Type**—Displays the MSTP type of the port.
  - *Boundary*—A Boundary port attaches MSTP bridges to a LAN in an outlying 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 bridge ID number that connects the link or shared LAN to the root.
- **Designated Port ID**—Displays the priority and port ID 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.
- **Remaining Hops**—Displays the hops remaining to the next destination.

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

13

MAC Address Tables

This chapter describes how to add MAC addresses to the switch and includes the following topics:

- Types of MAC Addresses
- Configuring Static MAC Addresses
- Configuring Static MAC Address Filter
- Configuring Dynamic MAC Address Aging Time
- Querying Dynamic MAC Addresses
- Configuring Reserved MAC Addresses

Types of MAC Addresses

There are two types of MAC addresses: static and dynamic. Depending on their type, MAC addresses are either stored in the Static Address table or in the Dynamic Address table, along with VLAN and port information.

Static addresses are configured by the user, and therefore, they do not expire. A new source MAC address that appears in a frame arriving at the switch is added to the Dynamic Address table. This MAC address is retained for a configurable period of time. If another frame with the same source MAC address does not arrive at the switch before that time period expires, the MAC entry is aged (deleted) from the table.

When a frame arrives at the switch, the switch searches for a corresponding or matching destination MAC address entry in the static or dynamic table. If a match is found, the frame is marked for egress on the port specified in the table. If frames are sent to a MAC address that is not found in the tables, they are transmitted or broadcast to all ports on the relevant VLAN. Such frames are referred to as unknown Unicast frames.

Configuring Static MAC Addresses

Static MAC addresses are assigned to a specific physical interface and VLAN on the switch. If that address is detected on another interface, it is ignored, and is not written to the address table. Up to 256 static MAC addresses can be configured on the switch.

To define a static MAC address:

STEP 1 Click **MAC Address Tables** > **Static Address**.

STEP 2 To add a static MAC address, click **Add**.

STEP 3 Enter the following information:

- **VLAN ID**—Select an VLAN ID.
- **MAC Address**—Enter the MAC address.
- **Interface**—Select a port or LAG for the MAC address.
- **Status**—Select how the MAC address is treated. The options are:
  - *Permanent*—The switch never removes this MAC address. If the static MAC address is saved to the Startup Configuration, it is retained after rebooting.
  - *Delete on Reset*—The static MAC address is deleted when the switch is reset.
  - *Delete on Timeout*—The MAC address is deleted when aging occurs.
  - *Secure*—The MAC address is secure when the port is in classic locked mode.

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

Configuring Static MAC Address Filter

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:

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.

Configuring Dynamic MAC Address Aging Time

The Dynamic Address Table contains the MAC addresses acquired by monitoring the source addresses of traffic entering the switch. To prevent this table from overflowing and to make room for new MAC addresses, an address is deleted if no traffic is received for a certain period. This period of time is the aging interval.

To set the aging interval for dynamic MAC addresses:

STEP 1 Click **MAC Address Tables** > **Dynamic Address Settings**.

STEP 2 Enter the value in the **Aging Time** field. The aging time is a value between the user-configured value and twice of that value minus. For example, if you entered 300 seconds, the aging time is between 300 and 599 seconds.

STEP 3 Click **Apply**. The aging time is defined, and the Running Configuration is updated.

Querying Dynamic MAC Addresses

Use the Dynamic Address page to query the dynamic MAC addresses according to the following criteria:

- VLAN ID
- Interface
- MAC address

This page displays the dynamically learned MAC addresses. You can clear the dynamic addresses from the table and specify a query criteria to display a subset of the table, such as the MAC addresses learned on a specific interface. You can also specify how the query results are sorted. If no filter criteria is entered, the entire table is displayed.

To query dynamic addresses:

STEP 1 Click **MAC Address Tables** > **Dynamic Address**.

STEP 2 Enter the query criteria:

- **VLAN ID equals to** —Check and enter the VLAN ID for which the table is queried.
- **MAC Address equals to**—Check and enter the MAC address for which the table is queried.
- **Interface equals to**—Check and select the interface for which the table is queried. The query can search for specific port or LAG.

STEP 3 Click **Go**. The Dynamic Address Table is queried and the results are displayed.

STEP 4 If needed, select the key by which the table is sorted from the **Dynamic Address Table Sort Key** drop-down menu, and click **Go**. The address table will be sorted by VLAN ID, MAC address, or interface.

STEP 5 Click **Clear Table** to delete all dynamic MAC addresses.

Configuring Reserved MAC Addresses

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** > **Reserved MAC Address**.

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.
  - *Peer*—Drops or deals with the packet depending on the protocol.

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

14

Multicast Forwarding

This chapter describes the Multicast forwarding feature and includes the following topics:

Multicast Forwarding

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.

For Multicast forwarding to work across IP subnets, nodes, and routers must be Multicast-capable. A Multicast-capable node must be able to:

- Send and receive Multicast packets.
- Register the Multicast addresses being listened to by the node with local routers, so that local and remote routers can route the Multicast packet to the nodes.

Typical Multicast Setup

While Multicast routers route Multicast packets between IP subnets, Multicast-capable Layer 2 switches forward Multicast packets to registered nodes within a LAN or VLAN.

A typical setup involves a router that forwards the Multicast streams between private and/or public IP networks, a device with Internet Group Membership Protocol (IGMP) snooping capabilities, or Multicast Listener Discovery (MLD) snooping, and a Multicast client that wants to receive a Multicast stream. In this setup, the router sends IGMP queries periodically.

NOTE MLD for IPv6 is derived from the IGMP v2 for IPv4. Even though the description in this section is mostly for IGMP, it also describes coverage of MLD where implied. These queries reach the switch, which in turn floods the queries to the VLAN, and also learns the port where there is a Multicast router (Mrouter). When a host receives the IGMP query message, it responds with an IGMP Join message saying that the host wants to receive a specific Multicast stream and optionally from a specific source. The switch with the IGMP snooping analyzes the Join messages, and learns that the Multicast stream the host has requested must be forwarded to this specific port. It then forwards the IGMP Join to the Mrouter only. Similarly, when the Mrouter receives an IGMP Join message, it learns the interface from which it received the Join messages that wants to receive a specific Multicast stream. The Mrouter forwards the requested Multicast stream to the interface.

In a Layer 2 Multicast service, a Layer 2 switch receives a single frame addressed to a specific Multicast address. It creates copies of the frame to be transmitted on each relevant port.

When the switch is IGMP/MLD-snooping-enabled and receives a frame for a Multicast stream, it forwards the Multicast frame to all the ports that have registered to receive the Multicast stream using IGMP Join messages.

The switch can forward Multicast streams only based on Multicast MAC Group Address. It can be configured per VLAN.

The switch maintains lists of Multicast groups for each VLAN, and this manages the Multicast information that each port should receive. The Multicast groups and their receiving ports can be configured statically or learned dynamically using IGMP or Multicast Listener Discovery (MLD) protocols snooping.

Multicast registration is the process of listening and responding to Multicast registration protocols. The available protocols are IGMP for IPv4 and MLD for IPv6. When IGMP/MLD snooping is enabled in a device on a VLAN, it analyzes the IGMP/MLD packets it receives from the VLAN connected to the device and Multicast routers in the network.

When a device learns that a host is using IGMP/MLD messages to register to receive a Multicast stream, optionally from a specific source, the device adds the registration to its Multicast Forwarding Data Base (MFDB).

IGMP/MLD snooping can effectively reduce Multicast traffic from streaming bandwidth-intensive IP applications. A device using IGMP/MLD snooping only forwards Multicast traffic to the hosts interested in that traffic. This reduction of Multicast traffic reduces the packet processing at the device, and also reduces the workload of the end hosts, since they do not have to receive and filter all of the Multicast traffic generated in the network.

The following versions are supported:

- IGMP v1/v2/ v3
- MLD v1/v2
- A simple IGMP Snooping Querier

An IGMP Querier is required to facilitate the IGMP protocol on a given subnet. In general, a Multicast router is also an IGMP Querier. When there are multiple IGMP Queriers in a subnet, the queriers elect a single querier as the primary querier.

The switch can be configured to be an IGMP Querier as a backup querier, or in situation where a regular IGMP Querier does not exist. The switch is not a full capability IGMP Querier.

If the switch is enabled as an IGMP Querier, it starts after a quarter of query interval have passed with no IGMP traffic (queries) detected from a Multicast router. In the presence of other IGMP Queriers, the device might (or might not) stop sending queries, based on the results of the standard querier selection process.

Multicast Address Properties

Multicast addresses have the following properties:

- Each IPv4 Multicast address is in the address range 224.0.0.0 to 239.255.255.255.
- The IPv6 Multicast address is FF00:/8.
- To map an IP Multicast group address to an Layer 2 Multicast address:

- For IPv4, this is mapped by taking the 23 low-order bits from the IPv4 address, and adding them to the 01:00:5e prefix. By standard, the upper nine bits of the IP address are ignored, and any IP addresses that only differ in the value of these upper bits are mapped to the same Layer 2 address, since the lower 23 bits that are used are identical. For example, 234.129.2.3 is mapped to a MAC Multicast group address 01:00:5e:01:02:03. Up to 32 IP Multicast group addresses can be mapped to the same Layer 2 address.
- For IPv6, this is mapped by taking the 32 low-order bits of the Multicast address, and adding the prefix of 33:33. For example, the IPv6 Multicast address FF00:1122:3344 is mapped to Layer 2 Multicast 33:33:11:22:33:44.

Configuring Multicast Properties

Use the Properties page to globally enable IGMP Snooping and/or IPv6 MLD Snooping on the switch and set the default action for unknown Multicast traffic. By default, all Multicast frames are flooded to all ports of the VLAN.

To configure Multicast properties:

STEP 1 Click **Multicast** > **Properties**.

STEP 2 Enter the following information:

- **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 Multicast properties are defined, and the Running Configuration is updated.

Configuring IP Multicast Group Addresses

Use the IP Multicast Group Address page to query and add IP Multicast groups.

To define and view IP Multicast groups:

STEP 1 Click **Multicast** > **IP Multicast Group Address**.

STEP 2 Enter the query criteria:

- **VLAN ID equals to**—Define the VLAN of the group to be displayed.
- **IP Version equals to**—Select either **Version 4** or **Version 6**.
- **IP Multicast Group Address equals to**—Define the IP address of the Multicast group to be displayed.

STEP 3 Click **Go**. The IP Multicast group addresses that match the criteria are displayed.

STEP 4 To add a static IP Multicast group address, click **Add**.

NOTE Member ports for a static IP multicast group address can be configured statically only.

STEP 5 Enter the following information:

- **VLAN ID**—Select the VLAN for the group to be added.
- **IP Version**—Select either **Version 4** or **Version 6**.
- **IP Multicast Group Address**—Enter the IP address of the new Multicast group.

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 IP Multicast group address is added, and the Running Configuration is updated.

Configuring IGMP Snooping

To support selective Multicast forwarding (IPv4), IGMP Snooping must be enabled globally and for each relevant VLAN.

By default, the switch forwards Multicast frames to all ports of the relevant VLAN, essentially treating the frame as if it is a Broadcast. With IGMP Snooping, the switch forwards Multicast frames to the ports that have registered Multicast clients.

NOTE The switch supports IGMP Snooping on both static and dynamic VLANs.

When IGMP Snooping is enabled globally or on a VLAN, all IGMP packets are forwarded to the CPU. The CPU analyzes the incoming packets, and determines the following:

- Which ports are asking to join which Multicast groups on what VLAN.
- Which ports are connected to Multicast routers (Mrouters) that are generating IGMP queries.
- Which ports are receiving PIM, OSFP, DVMRP, or IGMP query protocols.

Ports asking to join a specific Multicast group issue an IGMP report that specifies which group the host wants to join. This results in the creation of a forwarding entry in the Multicast forwarding database.

The IGMP Snooping Querier is used to support a Layer 2 Multicast domain of snooping switches in the absence of a Multicast router. For example, where Multicast content is provided by a local server, but the router (if one exists) on that network does not support Multicast.

There should be only one IGMP querier in a Layer 2 multicast domain. The switch supports standards-based IGMP querier election when more than one IGMP querier is present in the domain.

To configure general IGMP Snooping parameters and enable IGMP Snooping on a VLAN:

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 Select a VLAN, and click **Edit**.

STEP 4 Enter the following information:

- **VLAN ID**—Select the VLAN ID where IGMP Snooping is defined.
- **IGMP Snooping Status**—Enable or disable the monitoring of network traffic to determine which hosts have asked to be sent Multicast traffic.
- **MRouter Ports Auto Learn**—Enable or disable auto learning of the ports to which the Mrouter is connected.
- **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**—Enter the number of IGMP group-specific queries sent before the switch assumes there are no more members for the group, if the switch 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**—Enable the immediate leave to decrease the time it takes to block a Multicast stream sent to a member port when an IGMP group leave message is received on that port.
- **IGMP Querier Status**—Enable or disable the IGMP querier.

  There should be only one IGMP querier in a network. The switch supports standards-based IGMP querier election. Some of the values of the operational parameters of this table are sent by the elected querier. The other values are derived from the switch.
- **IGMP Querier Version**—Select the IGMP version used if the switch becomes the elected querier. Select IGMPv3 if there are switches and/or Multicast routers in the VLAN that perform source-specific IP Multicast forwarding.

STEP 5 Click **Apply**. The IGMP Snooping settings are defined, and the Running Configuration is updated.

Configuring MLD Snooping

To support selective Multicast forwarding (IPv6), MLD Snooping must be enabled globally and for each relevant VLAN. The switch supports MLD Snooping on both static and dynamic VLANs.

Hosts use the MLD protocol to report their participation in Multicast sessions, and the switch uses MLD Snooping to build Multicast membership lists. It uses these lists to forward Multicast packets only to switch ports where there are host nodes that are members of the Multicast groups. The switch does not support MLD querier.

The switch supports two MLD Snooping versions:

- MLDv1 Snooping detects MLDv1 control packets, and sets up traffic bridging, based on IPv6 destination Multicast addresses.

- MLDv2 Snooping uses MLDv2 control packets to forward traffic based on the destination IPv6 Multicast address only. It supports the capability to resolve the MLDv2 control packets.

The actual MLD version is selected by the Multicast router in the network.

In an approach similar to IGMP Snooping, MLD frames are snooped as they are forwarded by the switch from stations to an upstream Multicast router and vice versa. This facility enables a switch to conclude the following:

- On which ports stations interested in joining a specific Multicast group are located
- On which ports Multicast routers sending Multicast frames are located

This knowledge is used to exclude irrelevant ports (ports on which no stations have registered to receive a specific Multicast group) from the forwarding set of an incoming Multicast frame.

If you enable MLD Snooping in addition to the manually configured Multicast groups, the result is a union of the Multicast groups and port memberships derived from the manual setup and the dynamic discovery by MLD Snooping. However, only the static definitions are preserved when the switch is rebooted.

To enable MLD Snooping:

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

STEP 2 Enter the following information:

- **MLD Snooping Version**—Select either MLDv1 or MLDv2.
- **Report Suppression**—Enable or disable MLD Snooping report suppression. Disabling this feature will forward all MLDv1 reports to Multicast routers.

STEP 3 Click **Apply**.

STEP 4 Select a VLAN, and click **Edit**.

STEP 5 Enter the following information:

- **VLAN ID**—Select the VLAN ID.
- **MLD Snooping Status**—Enable or disable MLD Snooping on the VLAN. The switch monitors network traffic to determine which hosts have asked to be sent Multicast traffic. The switch performs MLD Snooping only when MLD Snooping is enabled globally and on the VLAN.

- **MRouter Ports Auto Learn**—Enable or disable auto learning of the Multicast router.
- **Query Robustness**—Enter the robustness variable value to be used if the switch cannot read this value from messages sent by the elected querier.
- **Query Interval**—Enter the query interval value to be used by the switch if the switch cannot derive the value from the messages sent by the elected querier.
- **Query Max Response Interval**—Enter the query maximum response delay to be used if the switch cannot read the maximum response time value from general queries sent by the elected querier.
- **Last Member Query Counter**—Enter the last member query count to be used if the switch cannot derive the value from the messages sent by 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**—When enabled, reduces the time that it takes to block unnecessary MLD traffic sent to a switch port.

STEP 6 Click **Apply**. The Running Configuration is updated.

Querying IGMP/MLD IP Multicast Groups

The IGMP/MLD IP Multicast Group page displays the IPv4 and IPv6 group addresses that the switch learned from the IGMP/MLD messages that it snoops.

To query for an IP Multicast group:

STEP 1 Click **Multicast** > **IGMP/MLD IP Multicast Group**.

STEP 2 Enter the query criteria:

- **VLAN ID equals to**—Enter 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 3 Click **Go**. The following fields are displayed for each Multicast group:

- **VLAN ID**—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.
- **Life (sec)**—The dynamic group life time.

Configuring Multicast Router Ports

A Multicast router (Mrouter) port is a port that connects to a Multicast router. The switch includes the Mrouter port(s) when it forwards Multicast streams and IGMP/MLD registration messages. It is required in order for all Mrouters can, in turn, forward the Multicast streams and propagate the registration messages to other subnets.

Use the Multicast Router Port page to statically configure or see dynamically detected ports connected to Mrouters.

To define Multicast router ports:

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

STEP 2 Enter the query criteria:

- **VLAN ID equals to**—Select the VLAN ID for the router ports that are described.
- **IP Version equals to**—Select either **Version 4** or **Version 6** that the Multicast router supports.
- **Interface Type equals to**—Select the interface type (Port or LAG).

STEP 3 Click **Go**. The interfaces matching the query criteria are displayed.

STEP 4 For each interface, select its association type. The options are:

- **Static**—The port is statically configured as a Multicast router port.

- **Dynamic**—The port is dynamically configured as a Multicast router port by a MLD/IGMP query. To enable dynamic learning of Multicast router ports, go to the **IGMP Snooping** and **MLD Snooping** pages.
- **Forbidden**—This port is not to be configured as a Multicast router port, even if IGMP or MLD queries are received on this port.
- **None**—The port is not currently a Multicast router port.

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

Configuring Forward All Multicast

Use the Forward All page to configure the ports or LAGs to receive Multicast streams from a specific VLAN.

You can statically configure a port to Forward All if the devices connecting to the port do not support IGMP or MLD.

NOTE The configuration affects only the ports that are members of the selected VLAN.

To define Forward All Multicast:

STEP 1 Click **Multicast** > **Forward All**.

STEP 2 Define the VLAN ID, IP version, and port type for which Multicast traffic comes from, and click **Go**.

STEP 3 Select the interface that is to be defined as Forward All by using the following methods:

- **Static**—The port receives all registered Multicast streams.
- **Forbidden**—The port cannot receive any registered Multicast streams, even if IGMP/MLD snooping designated the port to join a Multicast group.
- **None**—The port is not currently a Forward All port.

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

Configuring Maximum IGMP and MLD 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 IGMP report was received when the limit is reached.

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

Configuring 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.

This section includes the following topics:

- **Configuring Multicast Filter Profiles**

- Configuring Interface Filter Settings

Configuring Multicast Filter 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 the profile IP group range.

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

Configuring Interface 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 IP version and 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.
- **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 is updated.

15

IP Configuration

IP interface addresses can be configured manually by the user, or automatically configured by a DHCP server.

This chapter provides information for defining the switch IP addresses, either manually or by making the switch a DHCP client.

It includes the following sections:

- **IP Addressing**
- **IPv4 Management and Interface**
- **IPv6 Management and Interface**
- **Configuring Domain Name System**

IP Addressing

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 Management and 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 **Administration** > **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:

- **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 Management and 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 **Administration** > **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.

Configuring Domain Name System

The Domain Name System (DNS) translates domain names into IP addresses for the purpose of locating and addressing hosts. As a DNS client, the switch resolves domain names to IP addresses through the use of one or more configured DNS servers.

This section describes how to define DNS servers and includes the following topics:

- **Configuring General DNS Settings**
- **Viewing Static and Dynamic DNS Servers**
- **Configuring Host Mapping**

Configuring General DNS Settings

Use the DNS Settings page to enable the DNS feature, configure the DNS servers, and set the default domain used by the switch.

To configure general DNS settings:

STEP 1 Click **IP Configuration** > **Domain Name System** > **DNS Settings**.

STEP 2 Check **Enable** next to the **DNS** field to designate the switch as a DNS client, which can resolve DNS names into IP addresses through one or more configured DNS servers.

STEP 3 If DNS is enabled, enter the DNS domain name used to complete unqualified host names in the **Default Domain Name** field. The switch appends this to all non-fully qualified domain names (NFQDNs) turning them into FQDNs.

NOTE Do not include the initial period that separates an unqualified name from the domain name (such as cisco.com).

STEP 4 Click **Apply**. The DNS parameters are defined, and the Running Configuration is updated.

STEP 5 Click **Details** next to next to the **DHCP Domain Search List** field to view the list of DNS servers configured on the switch, including the static DNS server added by the user and all dynamic DNS servers received from DHCPv4 and DHCPv6 servers.

STEP 6 To add a DNS server, click **Add**.

STEP 7 Enter the following information:

- **IP Version**—Select either **Version 6** or **Version 4**.
- **DNS Server IP Address**—Enter the IP address of the DNS server.
- **Preference**—Select the preference value for the DNS server. Each server has a preference value, a lower value means a higher chance of being used.

STEP 8 Click **Apply**. The DNS server is defined, and the Running Configuration is updated.

Viewing Static and Dynamic DNS Servers

The search list contains one static domain name defined by the user and dynamic domain names received from DHCPv4 and DHCPv6 servers.

To view the domain names that have been configured on the switch, click **IP Configuration** > **Domain Name System** > **Search List**.

The following fields are displayed:

- **Source**—Source of the server's IP address (static or DHCPv4 or DHCPv6) for this domain.
- **Preference**—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.
- **Domain Name**—Name of domain that can be used on the switch.

Configuring Host Mapping

Host name and IP address mappings are stored in the Host Mapping Table (DNS cache).

This cache contains the static entries (mapping pairs) that are manually added to the cache.

Name resolution always begins by checking static entries, and continues by sending requests to the external DNS server.

Up to eight IP addresses can be mapped to a host, but at present only the first IP-address-to-host mapping is applicable.

To add a host mapping:

STEP 1 Click **IP Configuration** > **Domain Name System** > **Host Mapping**.

The following fields are displayed:

- **Host Name**—User-defined host name or fully-qualified name.
- **IP Address**—The host IP address.
- **IP Version**—IP version of the host IP address.
- **Type**—Static entry to the cache.

- **Status—** Displays the results of attempts to access the host (always shows OK for static entries).

STEP 2 To add a host mapping, click **Add**.

STEP 3 Enter the following information:

- **IP Version**—Select either **Version 6** or **Version 4**.
- **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 through 9, the underscore and the hyphen. A period (.) is used to separate labels.
- **IP Address (es)**—Enter a single address or up to eight associated IP addresses (IPv4 or IPv6).

STEP 4 Click **Apply**. The host mapping is added, and the Running Configuration is updated.

16

Configuring Security

The Cisco 220 switch handles various types of security, such as permission to administer the switch, protection from attacks directed at the switch CPU, access control of end-users to the network through the switch, protection from other network users (prevent the attacks that pass through, but are not directed at, the switch).

This chapter describes various aspects of security and access control and includes the following topics:

- **Configuring Users**
- **Configuring TACACS+ Servers**
- **Configuring RADIUS Servers**
- **Configuring Management Access Methods**
- **Configuring Password Complexity Rules**
- **Configuring Management Access Authentication**
- **Configuring TCP/UDP Services**
- **Configuring Storm Control**
- **Configuring Port Security**
- **Configuring 802.1X**
- **Configuring DoS Protection**
- **Configuring DHCP Snooping**
- **Configuring IP Source Guard**
- **Configuring Dynamic ARP Inspection**

Configuring Users

The default username/password is **cisco/cisco**. The first time that you log in with the default username and password, or when the current password expires, you are required to set a new password. Password complexity is enabled by default.

Use the User Accounts page to add additional users that are permitted to manage the switch or to change the passwords of existing users.

NOTE The default user (**cisco**) cannot be deleted.

To add a new user:

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

The User Account Table displays all users defined on the switch and their privilege levels.

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

STEP 3 Enter the following information:

- **User Name**—Enter a new username between 0 and 32 alphanumeric characters.
- **Password**—Enter a password. The password must comply with the minimum strength and complexity requirements shown on the page.
- **Confirm Password**—Enter the password again.
- **Password Strength Meter**—Displays the strength of password. The rules for password strength and complexity are configured on the Password Strength page. See the **Configuring Password Complexity Rules** section for more details.
- **User Level**—Select the privilege level for the user.
  - *Read-Only CLI Access (1)*—User can only access the command-line interface (CLI) and perform the commands that do not change the switch configuration. User cannot access the web-based interface.
  - *Read/Write Management Access (15)*—User can access the web-based interface, and can configure the switch.

STEP 4 Click **Apply**. The user is added or modified, and the Running Configuration is updated.

Configuring TACACS+ Servers

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.

TACACS+ is supported only with IPv4.

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 In the **Use Default Parameters** area, specify the default TACACS+ parameters:

- **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.

- **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.

STEP 3 Click **Apply**. The TACACS+ default parameters are defined, and the Running Configuration is updated.

STEP 4 To add a TACACS+ server, click **Add**.

STEP 5 Enter the following information:

- **Server Definition**—Select whether to specify the TACACS+ server by IP address or name.
- **IP Version**—Select either **Version 4** or **Version 6** if the TACACS+ server is identified by IP address.
- **Server IP Address/Name**—Enter the IP address or hostname of the TACACS+ server.
- **Priority**—Enter the order that the TACACS+ server is used. Zero is the highest priority server and is the first server used. If it cannot establish a session with the highest priority server, the switch will try the next highest priority server.
- **Key String**—A key string is used to encrypt communications by using MD5. You can select **Use Default** to use the default key (defined under the TACACS+ default parameters), or you can select **User Defined (Encrypted)** or **User Defined (Plaintext)** to enter the key in encrypted or plaintext form. The key must match the encryption key configured on the TACACS+ server. 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.
- **Timeout for Reply**—Select **User Defined** to enter the amount of time that passes before the connection between the switch and the TACACS+ server times out, or select **Use Default** to use the default value.
- **Authentication IP Port**—Enter the port number through which the TACACS+ session occurs. The default is port 49.

STEP 6 Click **Apply**. The TACACS+ server is added, and the Running Configuration is updated.

Configuring RADIUS Servers

An organization can establish a Remote Authorization Dial-In User Service (RADIUS) server to provide a centralized 802.1X or MAC-based network access control for all of its devices. The switch can act as a RADIUS client that uses the RADIUS server to provide centralized security, authorization, and user authentication.

To use a RADIUS server, you should open an account for the switch on the RADIUS server, and configure that RADIUS server along with the other parameters on the RADIUS page.

NOTE If more than one RADIUS server has been configured, the switch uses the configured priorities of the available RADIUS servers to select the RADIUS server to be used by the switch.

To define the default RADIUS parameters and add a RADIUS server:

STEP 1 Click **Security** > **RADIUS**.

STEP 2 In the **Use Default Parameters** area, enter the default RADIUS parameters that are applied to all RADIUS servers. If a value is not entered for a specific server, the switch 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 switch waits for an answer from the RADIUS server before retrying the query, or switching to the next server.
- **Key String**—The key string is used to encrypt communications between the switch and the RADIUS server by using MD5. Enter the default key string in encrypted or plaintext form. This key must match the key configured on the RADIUS server. If you do not have an encrypted key string (from another device), enter the key string in plaintext form.

STEP 3 Click **Apply**. The default RADIUS parameters are defined, and the Running Configuration is updated.

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

STEP 5 Enter the following information:

- **Server Definition**—Select whether to specify the RADIUS server by IP address or name.

- **IP Version**—Select either **Version 4** or **Version 6** if the RADIUS server is identified by IP address.
- **Server IP Address/Name**—Enter the IP address or hostname of the RADIUS server.
- **Priority**—Enter the priority of the server. The priority determines the order that the switch attempts to contact the servers to authenticate users. The switch first starts with the highest priority server. Zero is the highest priority.
- **Key String**—Select **User Defined (Encrypted)** or **User Defined (Plaintext)** to enter the key string in encrypted or plaintext form used for authenticating and encrypting the communication between the switch and the RADIUS server. This key must match the key configured on the RADIUS server. You can also select **Use Default** to use the default key string.
- **Timeout for Reply**—Select **User Defined** to enter the number of seconds that the switch waits for an answer from the RADIUS server before retrying the query or switching to the next server, or select **Use Default** to use the default value.
- **Authentication IP Port**—Enter the UDP port number of the RADUS server port for authentication requests.
- **Retries**—Select **User Defined** to enter the number of requests that are sent to the RADIUS server before a failure is considered to have occurred, or select **Use Default** to use the default value.
- **Usage Type**—Select the RADIUS server authentication type. The options are:
  - *Login*—RADIUS server is used for authenticating users that want to administer the switch.
  - *802.1X*—RADIUS server is used for authentication in 802.1X access control.
  - *All*—RADIUS server is used for authenticating user that wants to administer the switch and for authentication in 802.1X access control.

STEP 6 Click **Apply**. The RADIUS server is added, and the Running Configuration is updated.

Configuring Management Access Methods

Management access authentication configures the authentication methods to be used to authenticate and authorize users from different management access methods (see **Configuring Management Access Authentication** for more details). Management access profiles limit management access from specific sources.

Only users who pass both the active access profile and management access authentication are given management access to the switch.

This section includes the following topics:

- **Access Profile Rules, Filters, and Elements**
- **Active Access Profile**
- **Configuring Access Profiles**
- **Configuring Profile Rules**

Access Profile Rules, Filters, and Elements

Access profiles consist of rules for allowing access to the switch. Each access profile can 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 switch:
  - Telnet
  - Secure Telnet (SSH)
  - Hypertext Transfer Protocol (HTTP)
  - Secure HTTP (HTTPS)
  - Simple Network Management Protocol (SNMP)
  - All of the above
- **Action**—Permits or denies access to an interface or source address.
- **Interface**—Which ports or LAGs are permitted to access or denied access to the web-based interface.

- **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 switch module only by using an HTTPS session, while another user group might be able to access the switch module by using both HTTPS and Telnet sessions.

Active Access Profile

The Access Profiles page displays the access profiles that are defined and enables selecting one access profile to be the active one. Only one access profile can be active on the switch and any attempt to access the switch must fit the rules in the active access profile.

When a user attempts to access the switch through an access method, the switch looks to see if the active access profile explicitly permits management access to the switch through this method. If no match is found, access is denied.

If a console-only access profile has been activated, the only way to deactivate it is through a direct connection from the management station to the physical console port on the switch.

After an access profile has been defined, additional rules can be added or edited on the Profiles Rules page. See **Configuring Profile Rules** for more details.

Configuring Access Profiles

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 are finished. To add additional rules to the profile, use the Profile Rules page.

To add an access profile or select a different active access profile:

STEP 1 Click **Security** > **Management Access Method** > **Access Profiles**.

The Access Profiles Table 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 selected profile as the active access profile.

NOTE A caution message appears if you selected Console Only. If you continue, you are immediately disconnected from the web-based interface and can only access the switch through the console port.

NOTE If you selected any other access profile, a caution message appears warning you that, depending on the selected access profile, you might be disconnected from the web-based interface.

STEP 3 To add a new access profile and one rule, click **Add**.

STEP 4 Enter the following information:

- **Access Profile Name**—Enter the access profile name.
- **Rule Priority**—Enter the rule priority. When the packet is matched to a rule, user groups are either granted or denied access to the switch. The rule priority is essential to matching packets to rules, as packets are matched on a first-match basis. One is the highest priority.
- **Management Method**—Select the management method for which the rule is defined. Users with this access profile can only access the switch by using the management method selected. The options are:
  - *All*—Assigns all management methods to the rule.
  - *Telnet*—Users requesting access to the switch, who meet the Telnet access profile criteria, are permitted or denied access.
  - *Secure Telnet (SSH)*—Users requesting access to the switch, who meet the SSH access profile criteria, are permitted or denied access.
  - *HTTP*—Assigns HTTP access to the rule. Users requesting access to the switch, who meet the HTTP access profile criteria, are permitted or denied.
  - *Secure HTTP (HTTPS)*—Users requesting access to the switch, who meet the HTTPS access profile criteria, are permitted or denied.
  - *SNMP*—Users requesting access to the switch, who meet 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 switch if the user matches the settings in the profile.
  - *Deny*—Denies access to the switch 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 the selected interface. You need to select a port or LAG from the **Interface** drop-down menu.

- **Applies to Source IP Address**—Select the type of source IP address to which the access profile applies. The options are:
  - *All*—Applies to all IP addresses.
  - *User Defined*—Applies to only those types of IP addresses defined in the fields.
- **IP Version**—Select either **Version 4** or **Version 6** to define the source IP address.
- **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**. The access profile is created, and the Running Configuration is updated.

Configuring Profile Rules

Access profiles can contain multiple rules to determine who is permitted to manage and access the switch, and the access methods that may be used.

Each rule in an access profile contains an action and a 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 switch from all IP addresses except IP addresses that are allocated to the IT management center. In this way, the switch can still be managed and has gained another layer of security.

To add rules to an access profile:

STEP 1 Click **Security** > **Management Access Method** > **Profile Rules**.

STEP 2 Select an access profile, and click **Go**.

STEP 3 To add a rule for the selected access profile, click **Add**.

STEP 4 Enter the following information:

- **Access Profile Name**—Select an access profile to be configured.
- **Rule Priority**—Enter the rule priority. When the packet is matched to a rule, user groups are either granted or denied access to the switch. The rule priority is essential to matching packets to rules, as packets are matched on a first-match basis. One is the highest priority.
- **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 switch, who meet the Telnet access profile criteria, are permitted or denied access.
  - *Secure Telnet (SSH)*—Users requesting access to the switch, who meet the Telnet access profile criteria, are permitted or denied access.
  - *HTTP*—Assigns HTTP access to the rule. Users requesting access to the switch, who meet the HTTP access profile criteria, are permitted or denied.
  - *Secure HTTP (HTTPS)*—Users requesting access to the switch, who meet the HTTPS access profile criteria, are permitted or denied.
  - *SNMP*—Users requesting access to the switch, who meet the SNMP access profile criteria are permitted or denied.
- **Action**—Select **Permit** to permit the users that attempt to access the switch by using the configured access method from the interface and IP source defined in this rule, or select **Deny** to deny access.
- **Applies to Interface**—Select the interface attached to the rule. The options are:
  - *All*—Applies to all interfaces.
  - *User Defined*—Applies only to a specific port or LAG. You need to select a port or LAG from the **Interface** drop-down menu.

- **Applies to Source IP Address**—Select the type of source IP address to which the access profile applies. The options are:
  - *All*—Applies to all IP addresses.
  - *User Defined*—Applies to only those types of IP addresses defined in the fields.
- **IP Version**—Select either **Version 4** or **Version 6** to define the source IP address.
- **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 field:
  - *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**. The profile rule is added to the access profile, and the Running Configuration is updated.

Configuring Password Complexity Rules

Passwords are used to authenticate users accessing the switch. Simple passwords are potential security hazards. Therefore, password complexity requirements are enforced by default and may be configured as necessary.

Use the Password Strength page to modify the minimum password complexity requirements and set the password aging time.

To define the minimum password complexity requirements:

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

STEP 2 Enter the password aging parameters:

- **Password Aging**—Check **Enable** to ask the user to change the password when the Password Aging Time expires.

- **Password Aging Time**—Enter the number of days that can elapse before the user will be prompted to change the password.

  NOTE Password aging also applies to zero-length passwords (no password).

- **Password Complexity Settings**—Check **Enable** to enable complexity rules for passwords. If password complexity is enabled, passwords must conform to the following default settings:

  - Are different from the current password.
  - Are different from the current user name.
  - Contain characters from at least three character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard).
  - Contain no character that is repeated more than three times consecutively.
  - Have a minimum length of eight characters.

STEP 3 You can modify the default password settings in the following fields:

- **Minimal Password Length**—Enter the minimal number of characters required for passwords.

  NOTE A zero-length password (no password) is allowed, and can still have password aging assigned to it.

- **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 lowercase, uppercase, digits, and symbols or special characters.
- **The New Password Must Be Different than the Current One**—If selected, the new password cannot be the same as the current password upon a password change.
- **The New Password Must Be Different than the User Name**—If selected, the new password cannot be the same as the current username upon a password change.

STEP 4 Click **Apply**. The password complexity settings are defined, and the Running Configuration is updated.

Configuring Management Access Authentication

You can assign authentication methods to the various management access methods, such as SSH, console, Telnet, HTTP, and HTTPS. This authentication can be performed locally or on an external server, such as a TACACS+ or a RADIUS server.

For the RADIUS server to grant access to the web-based interface, the RADIUS server must return cisco-avpair = shell:priv-lvl=15.

User authentication occurs in the order that the authentication methods are selected. If the first authentication method is not 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 do not reply, the user is authenticated locally.

If an authentication method fails or the user has insufficient privilege level, the user is denied access to the switch. In other words, if authentication fails at an authentication method, the switch stops the authentication attempt; it does not continue and does not attempt to use the next authentication method.

To define authentication methods for an access method:

STEP 1 Click **Security** > **Management Access Authentication**.

STEP 2 Select an access method from the **Application** drop-down menu.

STEP 3 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. The applicable authentication methods are:

- **RADIUS**—User is authenticated on a RADIUS server. You must have configured one or more RADIUS servers.
- **TACACS+**—User is authenticated on a TACACS+ server. You must have configured one or more TACACS+ servers.
- **None**—User is allowed to access the switch without authentication.

- **Local**—Username and password are checked against the data stored on the local switch. These username and password pairs are defined on 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 4 Click **Apply**. The selected authentication methods are associated with the access method, and the Running Configuration is updated.

Configuring TCP/UDP Services

Use the TCP/UDP Services page to enable or disable TCP or UDP-based services on the switch, usually for security reasons. The active TCP and UDP connections are also displayed on the page.

To configure TCP/UDP services:

STEP 1 Click **Security** > **TCP/UDP Services**.

The **TCP Service Table** displays the following information for all active TCP connections:

- **Service Name**—Address method through which the switch is offering the TCP service.
- **Type**—IP protocol type that the service uses.
- **Local IP Address**—Local IP address through which the switch is offering the service.
- **Local Port**—Local TCP port through which the switch 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**—The state of the service. The optional values are:
  - *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 for all active UDP connections:

- **Service Name**—Access method through which the switch is offering the UDP service.
- **Type**—IP protocol that the service uses.
- **Local IP Address**—Local IP address through which the switch is offering the service.

TIP **Local Port**—Local UDP port through which the switch is offering the service.

STEP 2 If needed, enable or disable the following TCP/UDP services on the switch:

- **HTTP Service**—Check **Enable** to enable the HTTP service, or uncheck to disable it. The default is enabled.
- **HTTPS Service**—Check **Enable** to enable the HTTPS service, or uncheck to disable it. The default is enabled.
- **SNMP Service**—Check **Enable** to enable the SNMP service, or uncheck to disable it. The default is disabled.

- **Telnet Service**—Check **Enable** to enable the Telnet service, or uncheck to disable it. The default is disabled.
- **SSH Service**—Check **Enable** to enable the SSH service, or uncheck to disable it. The default is disabled.

STEP 3 Click **Apply**. The services are enabled or disabled, and the Running Configuration is updated.

Configuring Storm Control

When Broadcast, unknown 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 storm.

Storm protection enables you to limit the number of frames entering the switch and to define the types of frames that are counted towards this limit.

When the rate of Broadcast, unknown Multicast, or unknown Unicast frames is higher than the user-defined threshold, frames received beyond the threshold are discarded or the interface shuts down.

To define Storm Control:

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 To modify the storm control settings for a port, select the desired port and click **Edit**.

STEP 5 Enter the following information:

- **Interface**—Select the port to be defined.
- **Storm Control**—Enable or disable storm control on the port.
- **Unknown Unicast**—Enable or disable storm control for unknown Unicast traffic. It will count unknown Unicast traffic towards the bandwidth threshold.
- **Storm Control Rate Threshold**—Enter the maximum rate at which unknown Unicast packets can be forwarded. The default for this threshold is 10,000.
- **Unknown Multicast**—Enable or disable storm control for unknown Multicast traffic. It will count unknown Multicast traffic towards the bandwidth threshold.
- **Storm Control Rate Threshold**—Enter the maximum rate at which unknown Multicast packets can be forwarded. The default for this threshold is 10,000.
- **Broadcast**—Enable or disable storm control for Broadcast traffic. It will count Broadcast traffic towards the bandwidth threshold.
- **Storm Control Rate Threshold**—Enter the maximum rate at which Broadcast packets can be forwarded. The default for this threshold is 10,000.
- **Action**—Select the action when the rate of Broadcast, unknown Multicast, or unknown Unicast frames is higher than the user-defined threshold. The options are:
  - *Drop*—Discard the frames received beyond the threshold.
  - *Shutdown*—Shut down the port.

STEP 6 Click **Apply**. The port's storm control settings are modified, and the Running Configuration is updated.

Configuring Port Security

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 switch learns up to the maximum number of addresses allowed on the port (defined by Max No. of Addresses Allowed). The learned addresses are not subject to aging or relearning.
- **Limited Dynamic Lock**—The switch learns MAC addresses up to the configured limit of allowed addresses. After the limit is reached, the switch does not learn additional addresses. In this mode, the addresses are subject to aging and relearning.

When a frame with a new MAC address is detected on a port where it is not authorized (the port is classically locked and the new MAC address of this frame is learned on another classically locked port, or the port is dynamically locked and the maximum number of allowed addresses has been exceeded), the protection function 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 handled with the specified violation action, and the MAC address is not learned on that port.

Use the Port Security page to configure the security parameters for all ports, and to enable their modification.

To configure port security:

STEP 1 Click **Security** > **Port Security**.

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

STEP 3 Enter the following information:

- **Interface Status**—Check **Lock** to lock the port.
- **Learning Mode**—Select the type of port locking. This 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 interface immediately. But if the number of addresses that have already been learned exceeds the Max No. of Addresses Allowed, all learned addresses will be cleared.
  - *Limited Dynamic Lock*—Locks the interface by deleting the current dynamic MAC addresses associated with the interface. The interface learns up to the maximum addresses allowed on the interface. Both re-learning 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 interface if Limited Dynamic Lock learning mode is selected. The range is 1 to 256 and the default is 1.
- **Action on Violation**—If Interface Status is locked, select an action to be applied to packets arriving on a locked interface. 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, shuts down the interface, logs the events, and sends traps to the specified trap receivers. The interface remains shut down until reactivated, or until the switch is rebooted.
- **Trap Frequency**—Enter the minimum time in seconds that elapses between traps. The switch enables traps when a packet is received on a locked interface. This is relevant for lock violations.

STEP 4 Click **Apply**. Port security is modified, and the Running Configuration is updated.

Configuring 802.1X

Port-based access control has the effect of creating two types of access on the switch ports. One point of access enables uncontrolled communication, regardless of the authorization state (uncontrolled port). The other point of access authorizes communication between a host and the switch.

The 802.1x is an IEEE standard for port-based network access control. The 802.1x framework enables a device (the supplicant) to request port access from a remote device (authenticator) to which it is connected. Only when the supplicant requesting port access is authenticated and authorized is it permitted to send data to the port. Otherwise, the authenticator discards the supplicant data unless the data is sent to a Guest VLAN.

Authentication of the supplicant is performed by an external RADIUS server through the authenticator. The authenticator monitors the result of the authentication.

In the 802.1x standard, a device can be a supplicant and an authenticator at a port simultaneously, requesting port access and granting port access. However, this device is only the authenticator, and does not take on the role of a supplicant.

The following varieties of 802.1X exist:

- Single session 802.1X:
  - Single-session/single host—In this mode, the switch, as an authenticator, supports a single 802.1x session and grants permission to use the port to the authorized supplicant. All access by other devices received from the same port are denied until the authorized supplicant is no longer using the port or the access is to the guest VLAN.
  - Single session/multiple hosts—This follows the 802.1x standard. In this mode, the switch as an authenticator allows any device to use a port as long as it has been granted permission.
- Multi-Session 802.1X—Every device (supplicant) connecting to a port must be authenticated and authorized by the switch (authenticator) separately in a different 802.1x session.

Dynamic VLAN Assignment (DVA)

Dynamic VLAN Assignment (DVA) is also referred to as RADIUS VLAN Assignment in this guide. When a port is DVA-enabled, the switch automatically adds the port as an untagged member of the VLAN that is assigned by the RADIUS server during the authentication process. The switch classifies untagged packets to the assigned VLAN if the packets originated from the devices or ports that are authenticated and authorized.

For a device to be authenticated and authorized at a port which is DVA-enabled:

- The RADIUS server must authenticate the device and dynamically assign a VLAN to the device.
- The assigned VLAN must not be the default VLAN on the switch.
- A RADIUS server must support DVA with RADIUS attributes tunnel-type (64) = VLAN (13), tunnel-media-type (65) = 802 (6), and tunnel-private group-id = a VLAN ID.

Guest VLAN

Guest VLAN provides access to services that do not require the subscribing devices or ports to be 802.1x authenticated and authorized.

- The Guest VLAN, if configured, is a static VLAN with the following characteristics.
- Must be manually defined from an existing static VLAN.
- Is automatically available only to unauthorized devices or ports of devices that are connected and Guest-VLAN-enabled.
- If a port is Guest-VLAN-enabled, the switch automatically adds the port as untagged member of the Guest VLAN when the port is not authorized, and removes the port from the Guest VLAN when the first supplicant of the port is authorized.
- The Guest VLAN cannot be used as the Voice VLAN and an unauthenticated VLAN.

802.1X Parameters Workflow

Define the 802.1X parameters as follows:

- Define 802.1X settings for each port by using the Edit Port Authentication page.

NOTE

- You can select the Guest VLAN field to have untagged incoming frames go to the guest VLAN.
- Define host authentication parameters for each port using the Port Authentication page.
- View 802.1X authentication history using the Authenticated Hosts page.

Defining 802.1X Properties

The 802.1X Properties page is used to globally enable 802.1X and define how ports will be authenticated. For 802.1X to function, it must be activated both globally and individually on each port.

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

STEP 2 Enter the parameters.

- **Port-Based Authentication**—Enable or disable port-based, 802.1X 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 is removed from the Guest VLAN.
- **Guest VLAN ID**—Select the guest VLAN from the list of VLANs.

STEP 3 Click **Apply**. The 802.1X properties are modified, and the Running Configuration file is updated.

Defining 802.1X Port Authentication

The Port Authentication page enables configuration of 802.1X parameters for each port.

NOTE A port with 802.1x defined on it cannot become a member of a LAG.

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

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 switch does not provide authentication services to the client through the interface.
  - *Auto*—Enables port-based authentication and authorization on the switch. The interface moves between an authorized or unauthorized state based on the authentication exchange between the switch 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 the guest VLAN from the list of VLANs.
  - Selected—Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the Guest VLAN IDfield in the 802.1X Port Authentication page. After an authentication failure, and ifGuest VLAN is activated globally on a given port, the guest VLAN is automatically assigned to the unauthorized ports as an Untagged VLAN.
  - Cleared—Disables Guest VLAN on the port.
- **Periodic Reauthentication**—Select to enable port re-authentication 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 re-authentication.
- **Authenticator State**—Displays the defined port authorization state.

NOTE If the port is not in Force-Authorized or Force-Unauthorized, it is 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 number of maximum of authenticated hosts allowed on the specific interface. This value only takes effect on multi-sessions mode.
- **Quiet Period**—Enter the number of seconds that the switch remains in the quiet state following a failed authentication exchange.
- **Resending EAP**—Enter the number of seconds that the switch 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 can be sent. If a response is not 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 switch resends a request to the authentication server.

STEP 4 Click **Apply**. The port settings are defined, and the Running Configuration file is updated.

Defining 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.

The 802.1X modes are:

- **Single**—Only a single authorized host can access the port.
- **Multiple Host**—Multiple hosts can be attached to a single 802.1X enabled port. Only the first host must be authorized, and then the port is open for all who want to access the network. If the host authentication fails, or an EAPOL-logoff message is received, all attached clients are denied access to the network.
- **Multiple Sessions**—Enables the number of specific authorized hosts to access the port. Each host is treated as if it was the first and only user and must be authenticated. Filtering is based on the source MAC address.

To define 802.1X advanced settings for ports:

STEP 1 Click **Security > 802.1X > Host and Session Authentication**.

The authentication parameters are described for all ports. All fields except **Number of Violation** are described in the **Edit** page. The **Number of Violation** field displays the number of packets that arrive on the interface in a single-host mode from a host for which the MAC address is not 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 one of the modes. These modes are described above in Defining Host and Session Authentication.

NOTE The following fields are only relevant if you select Single in the Host Authentication field.

- **Action on Violation**—Select the action to be applied to packets arriving in Single Session/Single Host mode, from a host whose MAC address is not 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 remains shut down until reactivated, or until the switch 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 defined, and the Running Configuration file is updated.

Viewing Authenticated Hosts

Click **Security** > **802.1X** > **Authenticated Hosts**.

The Authenticated Hosts page displays the following fields:

- **User Name**—Supplicant names that were authenticated on each port.
- **Port**—Number of the port.
- **Session Time (DD:HH:MM:SS)**—Amount of time that the supplicant was logged on the port.
- **Authentication Method**—Method by which the last session was authenticated.
- **MAC Address**—Displays the supplicant MAC address.
- **VLAN ID**—Displays the supplicant VLAN ID.

Configuring DoS Protection

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.

The DoS protection feature is a set of predefined rules that protect the network from malicious attacks. The DoS Security Suite Settings enables activating the security suite.

This section describes how to configure the DoS protection features and includes the following topics:

- **Secure Core Technology (SCT)**
- **Default Configuration**
- **Configuring DoS Security Suite Settings**
- **Configuring SYN Protection**

Secure Core Technology (SCT)

One method of resisting DoS attacks employed by the switch is the use of SCT. SCT is enabled by default on the switch 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 switch 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.

There are no interactions with other features.

SCT can be monitored on the Security > Denial of Service > Security Suite Settings page (by clicking the **Details** button).

Default Configuration

The DoS protection feature has the following defaults:

- The DoS protection feature is disabled on all ports by default.
- The DoS protection feature is enabled in security suite by default.

- SYN-FIN and SYN-RST protections are enabled by default.
- The default protection mode of SYN protection is Block and Report. The default threshold is 60 SYN packets per second. The default period of port recovery is 60 seconds.

Configuring DoS Security Suite Settings

Use the Security Suite Settings page to enable filtering of traffic. This protects the network from a DoS and DDoS attacks.

NOTE Before activating DoS protection, you must unbind all ACLs or advanced QoS policies that are bound to a port. ACL and advanced QoS policies are not active when a port has DoS protection.

To set global DoS protection settings and monitor SCT:

STEP 1 Click **Security** > **Denial of Service** > **Security Suite Settings**.

The **CPU Protection Mechanism** field displays **Enabled**, which indicates that SCT is enabled.

STEP 2 Click **Details** beside the **CPU Utilization** field to go to the CPU Utilization page and view CPU resource utilization information.

STEP 3 Click **Edit** beside the **TCP SYN Protection** field to go to the SYN Protection page and enable this feature. See **Configuring SYN Protection** for more details.

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 DoS protection security suite settings are defined, and the Running Configuration is updated.

Configuring DoS 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** > **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**—Shows whether the IP gratuitous ARP protection feature is enabled or disabled 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.

Configuring SYN Protection

The network ports might be used by hackers to attack the switch in a SYN attack, which consumes TCP resources (buffers) and CPU power.

Because 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, which creates a Denial of Service (DoS).

When using the SYN protection feature, the CPU counts the SYN packets ingressing from each network port to the CPU per second.

If the number is higher than the specific, user-defined threshold, a deny SYN with MAC-to-me rule is applied on the port. This rule is unbound from the port every user-defined interval (SYN Protection Period).

To configure the SYN Protection settings:

STEP 1 Click **Security** > **Denial of Service** > **SYN Protection**.

The SYN Protection Interface Table displays the following information:

- **Interface**—Shows the port ID.
- **Current State**—Shows whether the SYN Protection feature is enabled or disabled on the port.
- **Last Attack**—Shows the time of the last SYN flood attack detected on the port.

STEP 2 Enter the global SYN Protection parameters:

- **Block SYN-RST Packets**—Check **Enable** to enable the feature. All TCP packets with both SYN and RST flags are dropped on the ports that enabled DoS protection.
- **Block SYN-FIN Packets**—Check **Enable** to enable the feature. All TCP packets with both SYN and FIN flags are dropped on the ports that enabled DoS protection.
- **SYN Protection Mode**—Select one of the following protection modes:
  - *Disable*—The feature is disabled on the port.

- *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**—Enter the 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**—Enter the 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**. The SYN Protection global settings are defined, and the Running Configuration is updated.

Configuring 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.

NOTE DHCP Snooping is applicable only for the switch models with the country of destination (-CN).

This section includes the following topics:

Configuring 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.
- **Verify MAC Address**—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.

Configuring DHCP Snooping on VLANs

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:

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.

Configuring DHCP Snooping Trusted Interfaces

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 **Enable** 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.

Querying DHCP Snooping 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. The database can be queried by VLAN.
- **MAC Address**—Indicates the MAC addresses recorded in the DHCP database. The database can be queried by MAC address.
- **IP Address**—Indicates the IP addresses recorded in the DHCP database The database can be queried by IP address.
- **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.

Viewing Option 82 Statistics

To view DHCP Snooping Option 82 statistics:

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

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

The following DHCP Snooping Option 82 statistical information is displayed:

- **Interface**—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.

Configuring Option 82 Interface 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:

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:
  - *Drop*—Drops DHCP packets with Option 82 information.
  - *Keep*—Keeps DHCP packets with Option 82 information.
  - *Replace*—Replaces DHCP packets with Option 82 information.

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

Configuring Option 82 Port CID Settings

Use the Option82 Port CID Settings page to configure the Option 82 circuit-ID suboption.

To configure the Option 82 circuit-ID suboption:

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 64 ASCII characters (no spaces). When the Option 82 feature is enabled, the default circuit-ID suboption is the switch VLAN and port identifier, in the format of vlan-mod-port.

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

Configuring 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.

NOTE IP Source Guard is applicable only for the switch models with the country of destination (-CN).

This section includes the following topics:

- **Configuring IP Source Guard Interface Settings**
- **Querying IP Source Binding Database**

Configuring IP Source Guard Interface Settings

Use the Interface Settings page to enable IP Source Guard on the interfaces.

To enable IP Source Guard on an interface:

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 only 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.

Querying IP Source 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 number.

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 number.
- **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.

Configuring Dynamic ARP Inspection

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

NOTE Dynamic ARP Inspection is applicable only for the switch models with the country of destination (-CN).

This section describes how to configure ARP on the switch and includes the following topics:

- **ARP Cache Poisoning**
- **How ARP Prevents Cache Poisoning**
- **Interaction Between ARP Inspection and DHCP Snooping**
- **Workflow to Configure ARP Inspection**
- **Configuring ARP Inspection Properties**
- **Configuring ARP Inspection Trusted Interfaces**
- **Viewing ARP Inspection Statistics**
- **Configuring ARP Inspection VLAN Settings**

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 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 above.

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 in the Ethernet header against the destination interface's 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 1 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 5 seconds interval.

Workflow to Configure ARP Inspection

To configure ARP Inspection:

STEP 1 Enable ARP Inspection and configure various options on the Security > ARP Inspection > Properties page. See **Configuring ARP Inspection Properties** for more details.

STEP 2 Configure interfaces as ARP trusted or untrusted on the Security > ARP Inspection > Interface Settings page. See **Configuring ARP Inspection Trusted Interfaces** for more details.

STEP 3 Define the VLANs on which ARP Inspection is enabled on the Security > ARP Inspection > VLAN Settings page. See **Configuring ARP Inspection VLAN Settings** for more details.

STEP 4 View ARP Inspection statistical information on the Security > ARP Inspection > Statistics page. See **Viewing ARP Inspection Statistics** for more details.

Configuring ARP Inspection Properties

Use the Properties page to enable dynamic ARP Inspection on the switch and set ARP packet validation parameters.

To define ARP Inspection properties:

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.

Configuring ARP Inspection Trusted Interfaces

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 300 pps and the default is 15.

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

Viewing 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**.

The following information is displayed:

- **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.

Configuring 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:

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.

17

Access Control

The Access Control List (ACL) feature is part of the security functions. ACL definitions serve as one of the functions to define traffic flows that are given a specific quality of service (QoS). For more information see the **Quality of Service** chapter.

ACLs enable network managers to define patterns (filter and actions) for ingress traffic. Packets, entering the switch on a port or LAG with an active ACL, are either admitted or denied entry.

This chapter includes the following topics:

- **Access Control Lists**
- **Configuring MAC-based ACLs**
- **Configuring MAC-based ACEs**
- **Configuring IPv4-based ACLs**
- **Configuring IPv4-Based ACEs**
- **Configuring IPv6-based ACLs**
- **Configuring IPv6-based ACEs**
- **Configuring ACL Binding**

Access Control Lists

An Access Control List (ACL) is an ordered list of classification filters and actions. Each single classification rule, together with its action, is called an Access Control Element (ACE).

Each ACE is made up of filters that distinguish traffic groups and associated actions. A single ACL may contain one or more ACEs, which are matched against the contents of incoming frames. Either a DENY or PERMIT action is applied to frames whose contents match the filter.

The switch supports a maximum of 512 ACLs, and a maximum of 128 ACEs per ACL.

When a packet matches an ACE filter, the ACE action is taken and that ACL processing is stopped. If the packet does not match the ACE filter, the next ACE is processed. If all ACEs of an ACL have been processed without finding a match, and if another ACL exists, it is processed in a similar manner.

NOTE If no match is found to any ACE in all relevant ACLs, the packet is dropped (as a default action). Because of this default drop action you must explicitly add ACEs into the ACL to permit all traffic, including management traffic, such as Telnet, HTTP, or SNMP that is directed to the switch itself. For example, if you do not want to discard all the packets that do not match the conditions in an ACL, you must explicitly add a lowest priority ACE into the ACL that permits all the traffic.

If IGMP/MLD Snooping is enabled at a port bound with an ACL, add ACE filters in the ACL to forward IGMP/MLD packets to the switch. Otherwise, IGMP/MLD Snooping will fail at the port.

The order of the ACEs within the ACL is significant because they are applied in a first-fit manner. The ACEs are processed sequentially, starting with the first ACE.

ACLs can be used for security, for example by permitting or denying certain traffic flows, and also for traffic classification and prioritization in QoS advanced mode.

NOTE A port can be either secured with ACLs or configured with advanced QoS policy, but not both.

There can only be one ACL per port, with the exception that it is possible to associate both an IPv4-based ACL and an IPv6-based ACL with a single port.

To associate more than one ACL with a port, a policy with one or more class maps must be used (see **Configuring QoS Policies** in the **Configuring QoS Advanced Mode** section).

The following types of ACLs can be defined (depending on which part of the frame header is examined):

- **MAC-based ACL**—Examines Layer 2 fields only, as described in the **Configuring MAC-based ACLs** section.
- **IP ACL**—Examines the Layer 3 of IP frames, as described in the **Configuring IPv4-based ACLs** section.
- **IPv6 ACL**—Examines the Layer 3 of IPv4 frames, as described in the **Configuring IPv6-based ACLs** section.

If a frame matches the filter in an ACL, it is defined as a flow with the name of that ACL. In QoS advanced mode, these frames can be referred to using this flow name, and QoS can be applied to these frames (see **Configuring QoS Advanced Mode**).

Creating ACLs Workflow

To create ACLs and associate them with an interface, perform the following:

STEP 1 Create one or more of the following types of ACLs:

- MAC-based ACL on the MAC-Based ACL page and the MAC-Based ACE page. See **Configuring MAC-based ACLs** and **Configuring MAC-based ACEs** for more details.
- IPv4-based ACL on the IPv4-Based ACL page and the IPv4-Based ACE page. See **Configuring IPv4-based ACLs** and **Configuring IPv4-Based ACEs** for more details.
- IPv6-based ACL on the IPv6-Based ACL page and the IPv6-Based ACE page. See **Configuring IPv6-based ACLs** and **Configuring IPv6-based ACEs** for more details.

STEP 2 Associate the ACL with interfaces on the ACL Binding page. See **Configuring ACL Binding** for more details.

Modifying ACLs Workflow

An ACL can only be modified if it is not in use. The following describes the process of unbinding an ACL in order to modify it:

- If the ACL does not belong to a class map (in QoS advanced mode), but it has been associated with an interface, unbind it from the interface on the ACL Binding page. See **Configuring ACL Binding** for more details.
- If the ACL is part of the class map and not bound to an interface, then it can be modified.
- If the ACL is part of a class map contained in a policy bound to an interface, you must perform the chain of unbinding as follows:
  - Unbind the policy containing the class map from the interface on the Policy Binding page. See **Configuring Policy Binding** for more details.
  - Delete the class map containing the ACL from the policy. See **Configuring QoS Policies** for more details.
  - Delete the class map containing the ACL. See **Configuring Class Mapping** for more details.

Configuring MAC-based ACLs

MAC-based ACLs are used to filter traffic based on Layer 2 fields. MAC-based ACLs check all frames for a match.

MAC-based ACLs are defined on the MAC-Based ACL page. The rules are defined on the MAC-Based ACE page.

To define a MAC-based ACL:

STEP 1 Click **Access Control** > **MAC-Based ACL**.

The MAC-Based ACL Table displays all currently defined MAC-based ACLs.

STEP 2 To add a new MAC-based ACL, 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 added, and the Running Configuration is updated.

STEP 5 Click **MAC-Based ACE Table**.

The MAC-Based ACE page opens. You can view and/or add rules to this MAC-based ACL. See **Configuring MAC-based ACEs** for more details.

Configuring MAC-based ACEs

To add rules (ACEs) to a MAC-based ACL:

STEP 1 Click **Access Control** > **MAC-Based ACE**.

STEP 2 Select a MAC-based ACL, and click **Go**. All currently defined MAC-based ACEs in the ACL are listed.

STEP 3 To add a rule (ACE) for the selected ACL, click **Add**.

STEP 4 Enter the following information:

- **ACL Name**—Displays the name of the ACL to which the 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*—Forwards packets that meet the ACE criteria.
  - *Deny*—Drops packets that meet the ACE criteria.
  - *Shutdown*—Drops packets that meet the ACE criteria, and disables the port from where the packets were received. These ports can be reactivated on the Port Management > Error Recovery Settings page.
- **Destination MAC Address**—Select **Any** if all destination addresses are acceptable, or select **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 will 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. Setting a bit as **1** indicates not to care and **0** indicates to mask that value. For example, the value FFFFFF000000 indicates that only the first three bytes of the destination MAC address are used.

NOTE With a mask of 0000 0000 0000 0000 0000 0000 1111 1111 1111 1111 1111 1111 1111 1111, you match on the bits where there is 0 and do not match on the bits where there is 1. You need to translate the 1 to a decimal integer and you write 0 for each four zeros. In this example, because 1111 1111 = FF, the mask would be written as 000000FFFFFF.

- **Source MAC Address**—Select **Any** if all source addresses are acceptable, or select **User Defined** to enter a source address or a range of source addresses.
  - *Source MAC Address Value*—Enter the MAC address to which the source MAC address will 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 of the VLAN tag to match.
- **802.1p**—Check **Include** to use 802.1p, and enter the following fields:
  - *802.1p Value*—Enter the 802.1p value to be added to the VPT tag.
  - *802.1p Mask*—Enter the wildcard mask to be applied to the VPT tag.
- **Ethertype**—Enter the frame Ethertype to be matched.

STEP 5 Click **Apply**. The MAC-based ACE is defined, and the Running Configuration is updated.

Configuring IPv4-based ACLs

IPv4-based ACLs are used to check IPv4 packets, while other types of frames, such as ARPs, are not checked.

The following fields can be matched:

- IP protocol (by name for well known protocols or directly by value)
- Source/destination IP addresses (including wildcards)
- Source/destination ports for TCP/UDP traffic
- Flag values for TCP frames
- DSCP/IP-precedence value
- ICMP and IGMP type and code

NOTE ACLs are also used as the building elements of flow definitions for per-flow QoS handling (see **Configuring QoS Advanced Mode**).

IPv4-based ACLs are defined on the IPv4-Based ACL page. The rules are defined on the IPv4-Based ACE page.

IPv6-based ACLs are defined on the IPv6-Based ACL page.

To define an IPv4-based ACL:

STEP 1 Click **Access Control** > **IPv4-Based ACL**.

The IPv4-Based ACL Table displays all currently defined IPv4-based ACLs.

STEP 2 To add a new IPv4-based ACL, 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 defined, and the Running Configuration is updated.

STEP 5 Click **IPv4-Based ACE Table**.

The IPv4-Based ACE page opens. You can view and/or add rules to this IPv4-based ACL. See **Configuring IPv4-Based ACEs** for more details.

Configuring IPv4-Based ACEs

To add rules (ACEs) to an IPv4-based ACL:

STEP 1 Click **Access Control** > **IPv4-Based ACE**.

STEP 2 Select an ACL, and click **Go**. All currently defined IPv4-based ACEs for the selected ACL are displayed.

STEP 3 To add a rule (ACE) for the selected ACL, click **Add**.

STEP 4 Enter the following information:

- **ACL Name**—Displays the name of the ACL.
- **Priority**—Enter the priority. ACEs with higher priority are processed first.
- **Action**—Select the action assigned to the packet matching the ACE. The options are:
  - *Permit*—Forwards packets that meet the ACE criteria.
  - *Deny*—Drops packets that meet the ACE criteria.
  - *Shutdown*—Drops packet that meets the ACE criteria and disables the port to which the packet was addressed. Ports are reactivated on the Port Management > Error Recovery Settings page.
- **Protocol**—Creates an ACE based on a specific protocol or protocol ID.
  - **Any (IP)**—Select to accept all IP protocols.
  - **Select from list**—Select one of the following protocols from the drop-down menu:

    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 select **User Defined** to enter a source address or a range of source addresses.
  - *Source IP Address Value*—Enter the IP address to which the source IP address will be matched.
  - *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. Setting a bit as **1** indicates not to care and **0** indicates to mask that value.
- **Destination IP Address**—Select **Any** if all destination address are acceptable, or select **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 IP address will be matched.
  - *Destination IP Wildcard Mask*—Enter the mask to define a range of IP addresses.
- **Source Port**—Select one of the following:
  - *Any*—Match to all source ports.
  - *Single*—Enter a single TCP/UDP source port to which packets are matched. This field is active only if TCP or UDP is selected from the **Select from list** drop-down menu.

- *Range*—Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.

- **Destination Port**—Select one of the available values. (They are the same as for the **Source Port** field.)

  NOTE You must select an IP protocol for the ACE before you enter the source and destination ports.

- **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.

  - *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**—Select the service type of IP packets. The options are:

  - *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 IP protocol of the ACL is ICMP, select the ICMP message type used for filtering purposes. The options are:

  - *Any (IP)*—All message types are accepted.
  - *Select from list*—Select message type by name.
  - *ICMP Type to match*—Enter the number of message type to be used for filtering purposes.

- **ICMP Code**—The ICMP messages can have a code field that indicates how to handle the message. Select **Any** to accept all codes, or select **User Defined** to enter an ICMP code for filtering purposes.

STEP 5 Click **Apply**. The IPv4-based ACE is defined, and the Running Configuration is updated.

Configuring IPv6-based ACLs

Use the IPv6-Based ACL page to create IPv6-based ACLs, which check pure IPv6-based traffic. IPv6-based ACLs do not check IPv6-over-IPv4 or ARP packets.

NOTE ACLs are also used as the building elements of flow definitions for per-flow QoS handling (see **Configuring QoS Advanced Mode**).

To define an IPv6-based ACL:

STEP 1 Click **Access Control** > **IPv6-Based ACL**.

STEP 2 To add a new IPv6-based ACL, 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 defined, and the Running Configuration is updated.

STEP 5 Click **IPv6-Based ACE Table**.

The IPv6-Based ACE page opens. You can view and/or add rules to this IPv6-based ACL. See **Configuring IPv6-based ACEs** for more details.

Configuring IPv6-based ACEs

To add rules (ACEs) to an IPv6-based ACL:

STEP 1 Click **Access Control** > **IPv6-Based ACE**.

STEP 2 Select an IPv6-based ACL, and click **Go**. All currently defined IPv6-based ACEs for the selected ACL are displayed.

STEP 3 To add a rule (ACE) for the selected ACL, click **Add**.

STEP 4 Enter the following information:

- **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. The options are:
  - *Permit*—Forwards packets that meet the ACE criteria.
  - *Deny*—Drops packets that meet the ACE criteria.
  - *Shutdown*—Drops packets that meet the ACE criteria, and disables the port to which the packets were addressed. Such ports can be reactivated on the Port Management > Error Recovery Settings page.
- **Protocol**—Creates this ACE based on a specific protocol or protocol ID.
  - **Any (IP)**—Select to accept all IP protocols.
  - **Select from list**—Select one of the following protocols:

    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 were sent.

    UDP—User Datagram Protocol. Transmits packets but does not guarantee their delivery.

    ICMP—Matches packets to the Internet Control Message Protocol (ICMP).
  - **Protocol ID to match**—Enter the ID of the protocol to be matched.
- **Source IP Address**—Select **Any** if all source address are acceptable, or select **User Defined** to enter a source address or a range of source addresses.
  - *Source IP Address Value*—Enter the IP address to which the source IP address will 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 address are acceptable, or select **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 will be 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*—Enter a single TCP/UDP source port to which packets are matched. This field is active only if TCP or UDP is selected from the **Select from list** drop-down menu.
  - *Range*—Select a range of TCP/UDP source ports to which the packet is matched.
- **Destination Port**—Select one of the available values. (They are the same as for the **Source Port** field.)

  NOTE You must select an IPv6 protocol for the ACE before you configure the source and destination ports.
- **TCP Flags**—Select one of 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.
  - *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**—Select the service type of IP packets. The options are:
  - *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 will be used for filtering purposes. The options are:

- *Any (IP)*—All message types are accepted.
- *Select from list*—Select the message type by name from the drop-down list.

- *ICMP Type to match*—Enter the number of the message type that will be used for filtering purposes.

- **ICMP Code**—The ICMP messages may have a code field that indicates how to handle the message. Select **Any** to accept all codes, or select **User Defined** to enter an ICMP code for filtering purposes.

STEP 5 Click **Apply**. The IPv6-based ACE is defined, and the Running Configuration is updated.

Configuring ACL Binding

When an ACL is bound to an interface, its ACE rules are applied to packets arriving at that interface. Packets that do not match any of the ACEs in the ACL are matched to a default rule, whose action is to drop unmatched packets.

Although each interface can be bound to only one ACL, multiple interfaces can be bound to the same ACL by grouping them into a policy map, and binding that policy map to the interface.

After an ACL is bound to an interface, it cannot be edited, modified, or deleted until it is removed from all interfaces to which it is bound or in use.

NOTE It is possible to either bind an interface to a policy or to an ACL but both cannot be bound.

To bind an ACL to an interface:

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

STEP 2 Select the interface type (Port or LAG), and 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.
- **MAC ACL**—MAC-based ACLs that are bound to the interface (if any).
- **IPv4 ACL**—IPv4-based ACLs that are bound to the interface (if any).
- **IPv6 ACL**—IPv6-based ACLs that are bound to the interface (if any).

STEP 3 To unbind all ACLs from an interface, select the interface, and click **Clear**.

STEP 4 To bind the ACLs to an interface, select the desired interface, and click **Edit**.

STEP 5 Select one of the following:

- **Select MAC-Based ACL**—Select a MAC-based ACL to be bound to the interface.
- **Select IPv4-Based ACL**—Select an IPv4-based ACL to be bound to the interface.
- **Select IPv6-Based ACL**—Select an IPv6-based ACL to be bound to the interface.

STEP 6 Click **Apply**. The ACL binding setting is modified, and the Running Configuration is updated.

NOTE If no ACL is selected, the ACLs that are previously bound to the interface are unbound.

18

Quality of Service

The quality of service (QoS) feature is applied throughout the network to ensure that network traffic is prioritized according to required criteria and the desired traffic receives preferential treatment.

This chapter includes the following topics:

QoS Features and Components

The QoS feature is used to optimize network performance. QoS provides the classification of incoming traffic to traffic classes based on the following attributes:

- Device configuration
- Ingress interface
- Packet content
- Combination of these attributes

QoS includes the following:

- **Traffic Classification**—Classifies each incoming packet as belonging to a specific traffic flow, based on the packet contents and/or the port. The classification is done by ACL, and only traffic that meets the ACL criteria is subject to cost of service (CoS) or QoS classification.
- **Assignment to Hardware Queues**—Assigns incoming packets to forwarding queues. Packets are sent to a particular queue for handling as a

function of the traffic class to which they belong. See **Configuring QoS Queues**.

- **Other Traffic Class-Handling Attribute**—Applies QoS functions to various classes, including bandwidth management.

The QoS mode that is selected applies to all interfaces on the switch. The switch supports the following QoS modes:

- **Basic Mode**—Class of service (CoS).

  All traffic of the same class receives the same treatment, which is the single QoS action of determining the egress queue on the egress port, based on the indicated QoS value in the incoming frame. When operating in QoS basic mode, the switch trusts this external assigned QoS value. The external assigned QoS value of a packet determines its traffic class and QoS.

- **Advanced Mode**—Per-flow quality of service (QoS).

  In QoS advanced mode, a per-flow QoS consists of a class map and a policer:

  - A class map defines the kind of traffic in a flow, and contains one or more ACLs. Packets that match the ACLs belong to the flow.
  - A policer applies the configured QoS to a flow. The QoS configuration of a flow may consist of egress queue, the DSCP or CoS/802.1p value, and actions on out of profile (excess) traffic.

- **Disable Mode**—All traffic is mapped to a single best effort queue so that no type of traffic is prioritized over another.

NOTE Only a single mode can be active at a time. When the switch is configured to work in QoS advanced mode, the settings for QoS basic mode are not active and vice versa.

When the QoS mode is changed, the following occurs:

- When changing from QoS advanced mode to any other mode, policy profile definitions and class maps are deleted. ACLs bonded directly to interfaces remain bonded.
- When changing from QoS basic mode to QoS advanced mode, the QoS trust mode configuration in QoS basic mode is not retained.
- When disabling QoS, the shaper and queue setting (WRR/SP bandwidth setting) are reset to default values.

- All other user configurations remain intact.

Workflow to Configure QoS Settings

To configure the QoS parameters, perform the following:

STEP 1 Choose the QoS mode (basic, advanced, or disabled) for the switch, and assign each interface a default CoS priority as described in the **Configuring QoS Properties** section.

STEP 2 Assign the schedule method (Strict Priority or WRR) and bandwidth allocation for WRR to the egress queues as described in the **Configuring QoS Queues** section.

STEP 3 Designate an egress queue to each CoS/802.1p priority as described in the **Mapping CoS/802.1p to a Queue** section. If the switch is in CoS/802.1 trusted mode, all incoming packets will be put into the designated egress queues according to the CoS/802.1p priority in the packets.

STEP 4 Designate an egress queue to each IP precedence as described in the **Mapping IP Precedence to Queue** section.

STEP 5 Designate an egress queue to each IP DSCP/TC value on the DSCP to Queue page, as described in the **Mapping DSCP to Queue** section. If the switch is in DSCP trusted mode, incoming packets are put into the egress queues based on their DSCP/TC values.

STEP 6 Remark the CoS/802.1p priority, IP precedence, and/or DSCP value for egress traffic on a port. The CoS/802.1p priority and IP precedence, or the CoS/802.1p priority and the DSCP value can be remarked simultaneously, but the IP precedence and DSCP values cannot be remarked simultaneously.

- Remark the CoS/802.1p priority for egress traffic from each queue as described in the **Mapping Queues to CoS/802.1p** section.
- Remark the IP precedence for egress traffic from each queue as described in the **Mapping Queue to IP Precedence** section.
- Remark the DSCP value for egress traffic from each queue as described in the **Mapping Queue to DSCP** section.

STEP 7 Enter bandwidth and rate limits:

- Set ingress rate limit and egress shaping rate per port as described in the **Configuring Bandwidth** section.

- Set egress shaping per queue as described in the **Configuring Egress Shaping per Queue** section.
- Set VLAN ingress rate limit as described in the **Configuring VLAN Rate Limit** section.

STEP 8 Configure the selected mode by performing one of the following:

- Configure QoS basic mode as described in the **Configuring QoS Basic Mode** section.
- Configure QoS advanced mode as described in the **Configuring QoS Advanced Mode** section.

STEP 9 Activate the TCP congestion avoidance algorithm as described in the **Configuring TCP Congestion Avoidance** section.

Configuring QoS Properties

Use the QoS Properties page to configure the QoS mode for the switch, and define the default CoS priority for each interface.

To select the QoS mode and define the default CoS priority for each interface:

STEP 1 Click **Quality of Service** > **General** > **QoS Properties**.

STEP 2 Select the QoS mode (basic, advanced, or disabled) that will be active on the switch.

STEP 3 Click **Apply**. The QoS mode is defined, and the Running Configuration is updated.

STEP 4 The **Interface CoS Configuration Table** displays the default CoS value for each interface. To modify the interface's default CoS value, select the desired interface and click **Edit**.

STEP 5 Enter the following information:

- **Interface**—Select the interface to be configured.
- **Default CoS**—Select the default CoS value to be assigned for incoming packets (that do not have a VLAN tag). The range is 0 to 7.

  The default CoS value is applicable only if the switch is in QoS basic mode and CoS/802.1p is the trusted mode.

STEP 6 Click **Apply**. The interface's default CoS value is changed, and the Running Configuration is updated.

STEP 7 To restore the CoS value to factory defaults, check the interfaces and click **Restore Defaults**.

Configuring QoS Queues

The switch supports eight queues for each interface. Queue number 8 is the highest priority queue. Queue number 1 is the lowest priority queue.

There are two ways of determining how traffic in queues is handled, Strict Priority (SP) and Weighted Round Robin (WRR).

- **Strict Priority (SP)**—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, which provide 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).

The queuing modes can be selected on the Queue page. When the queuing mode is by Strict Priority, the priority sets the order in which queues are serviced, starting with queue_8 (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 is 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 SP queues is always sent before traffic from the WRR queues. After the SP queues have been emptied, traffic from the WRR queues is forwarded. (The relative portion from each WRR queue depends on its weight).

To select the priority method and enter WRR data:

STEP 1 Click **Quality of Service** > **General** > **Queue**.

STEP 2 Enter the following information:

- **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 are not empty, meaning that they have descriptors to egress. It happens only if 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 defined, and the Running Configuration is updated.

Mapping CoS/802.1p to a Queue

Use the CoS/802.1p to Queue page to map 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 will be the default CoS/802.1p priority assigned to the ingress ports.

802.1p Values (0 to 7, 7 being the highest)	Queue (8 queues, 8 being the highest priority)	Notes
0	2	Background
1	1	Best Effort
2	3	Excellent Effort
3	4	Critical Application LVS phone SIP

802.1p Values (0 to 7, 7 being the highest)	Queue (8 queues, 8 being the highest priority)	Notes
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, the queue schedule method, and bandwidth allocation, it is possible to achieve the desired QoS in a network.

The CoS/802.1p to Queue mapping is applicable only if one of the following exists:

- The switch is in QoS basic mode and the trusted mode is CoS/802.1p.
- The switch is in QoS advanced mode and the packets belong to flows that are CoS/802.1p trusted.

To map CoS values to egress queues:

STEP 1 Click **Quality of Service** > **General** > **CoS/802.1p to Queue**.

STEP 2 Enter the following information:

- **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. Eight egress queues are supported, where Queue 8 is the highest priority egress queue and Queue 1 is the lowest priority egress queue.

For each 802.1p priority, select the Output Queue to which it is mapped.

STEP 3 Click **Apply**. 802.1p priority values to queues are mapped, and the Running Configuration is updated.

STEP 4 Click **Restore Defaults** to restore the CoS/802.1p to Queue mappings to factory defaults.

Mapping IP Precedence to Queue

To map IP precedence to egress queue:

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

STEP 2 Select the egress queue to which the IP precedence is mapped. Eight egress queues are supported, where queue 8 is the highest priority egress queue and queue 1 is the lowest priority egress queue.

STEP 3 Click **Apply**. IP precedence values to queues are mapped, and the Running Configuration is updated.

STEP 4 Click **Restore Defaults** to restore the IP Precedence to Queue mappings to factory defaults.

Mapping DSCP to Queue

Use the DSCP to Queue page to map IP DSCP to egress queues. The DSCP to Queue table determines the egress queues of the incoming IP packets based on their DSCP values. The original VLAN Priority Tag (VPT) of the packet is unchanged.

It is possible to achieve the desired QoS in a network by simply changing the DSCP to Queue mapping, the queue schedule method, and bandwidth allocation.

The DSCP to Queue mapping is applicable to IP packets if one of the following exists:

- The switch is in QoS basic mode and DSCP is the trusted mode.
- The switch is in QoS advanced mode and the packets belong to flows that are DSCP trusted.

Non-IP packets are always classified to the best-effort queue.

To map DSCP values to queues:

STEP 1 Click **Quality of Service** > **General** > **DSCP to Queue**.

The **Ingress DSCP** column displays the DSCP value in the incoming packet and its associated class.

STEP 2 Select the traffic forwarding queue from the **Output Queue** drop-down menu to which the DSCP value is mapped.

STEP 3 Click **Apply**. DSCP values to queues are mapped, and the Running Configuration is updated.

STEP 4 Click **Restore Defaults** to restore the DSCP to Queue mappings to factory defaults.

Mapping Queues 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:

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

STEP 2 For each output queue, select the CoS/802.1p priority to which egress traffic from the queue is remarked.

STEP 3 Click **Apply**. The Running Configuration is updated.

STEP 4 Click **Restore Defaults** to restore the Queue to CoS/802.1p mappings to factory defaults.

Mapping Queue to IP Precedence

To map egress queue to IP precedence:

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

STEP 2 For each output queue, select the IP precedence to which egress traffic from the queue is remarked.

STEP 3 Click **Apply**. The Running Configuration is updated.

STEP 4 Click **Restore Defaults** to restore the queue to IP precedence mappings to factory defaults.

Mapping Queue to DSCP

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

To map queues to DSCP values:

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

STEP 2 For each output queue, select the DSCP value to which egress traffic from the queue is remarked.

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

STEP 4 Click **Restore Defaults** to restore the queue to DSCP mappings to factory defaults.

Configuring Interface Remark

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 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 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.

Configuring Bandwidth

Use the Bandwidth page to define two sets of values that determine how much traffic the switch can receive and send.

The ingress rate limit is the number of bits per second that can be received from the ingress interface. Excess bandwidth above this limit is discarded.

To enter bandwidth limitation:

STEP 1 Click **Quality of Service** > **General** > **Bandwidth**.

STEP 2 To limit the bandwidth on a port, select the port and click **Edit**.

STEP 3 Enter the following information:

- **Interface**—Select the port to be configured.
- **Ingress Rate Limit**—Check **Enable** to enable the ingress rate limit, and enter the maximum amount of bandwidth allowed on the port in the **Ingress Rate Limit** field.
- **Egress Shaping Rates**—Check **Enable** to enable egress shaping on the port, and enter the maximum bandwidth for the egress interface in the **Committed Information Rate (CIR)** field.

STEP 4 Click **Apply**. The bandwidth settings are modified, and the Running Configuration is updated.

Configuring Egress Shaping per Queue

In addition to limiting transmission rate per port, which is done on the Bandwidth page, the switch 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 switch limits all frames except for management frames. Any frames that are not limited are ignored in the rate calculations, meaning that their size is not included in the limit total.

Per-queue egress rate shaping can be disabled.

This feature requires that the switch is in QoS basic mode or in QoS advanced mode.

To define egress shaping per queue:

STEP 1 Click **Quality of Service** > **General** > **Egress Shaping Per Queue**.

STEP 2 To shape the egress for up to eight queues on each interface, select the interface and click **Edit**.

STEP 3 Enter the following information:

- **Queue *x***—Check **Enable** to enable egress shaping on the queues.
- **Committed Information Rate (CIR)**—Enter the maximum rate (CIR) in kilobits per second (Kbps). CIR is the average maximum amount of data that can be sent.

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

Configuring VLAN Rate Limit

Rate limiting per VLAN, performed on the VLAN Ingress Rate Limit page, enables traffic limiting on VLANs. QoS rate limiting (configured on the Policy Table page) has priority over VLAN rate limiting. 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.

When VLAN ingress rate limiting is configured, it limits aggregate traffic from all ports on the switch.

VLAN rate limiting is configured at the device level and rate limits are applied independently for each device in the network. If there is more than one device in the system, the configured VLAN rate limit values will be applied on each of the devices independently.

This feature requires that the switch is in QoS basic mode or in QoS advanced mode.

To define the VLAN ingress rate limit:

STEP 1 Click **Quality of Service** > **General** > **VLAN Ingress Rate Limits**.

STEP 2 Click **Add**.

STEP 3 Enter the following information:

- **VLAN ID**—Select a VLAN.
- **Committed Information Rate (CIR)**—Enter the average maximum amount of data that can be accepted into the VLAN in kilobytes per second.

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

Configuring VLAN Port 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.

This feature requires that the switch is in QoS basic mode or in QoS advanced mode.

If both bandwidth limitation and VLAN port ingress rate limit are enabled at the same time, the smaller setting will take precedence.

To define the VLAN port ingress rate limit:

STEP 1 Click **Quality of Service** > **General** > **VLAN Port Ingress Rate Limits**.

STEP 2 Click **Add**.

STEP 3 Enter the following information:

- **VLAN ID**—Select a VLAN.
- **Committed Information Rate (CIR)**—Enter the average maximum amount of data that can be accepted into the specified interfaces in kilobytes 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 Running Configuration is updated.

Configuring TCP Congestion Avoidance

Use the TCP Congestion Avoidance page to activate the 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:

STEP 1 Click **Quality of Service** > **General** > **TCP Congestion Avoidance**.

STEP 2 Enable or disable TCP congestion avoidance.

STEP 3 Click **Apply**. The Running Configuration is updated.

Configuring 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.

To configure QoS basic mode, perform the following:

STEP 1 Select the QoS basic mode for the switch as described in the **Configuring QoS Properties** section.

STEP 2 Select the trust behavior as described in the **Configuring Basic QoS Trust Mode** section. The switch supports four trusted modes: CoS/802.1p, DSCP, IP precedence, and CoS/802.1p-DSCP. CoS/802.1p trusted mode uses the 802.1p priority in the VLAN tag. DSCP trusted mode use the DSCP value in the IP header.

STEP 3 If there is any port that, as an exception, should not trust the incoming CoS mark, disable the QoS state on that port on the Interface Settings page, as described in the **Configuring Basic QoS Interface Settings** section.

Enable or disable the global selected trusted mode at the ports on the Interface Settings page. If a port is disabled without trusted mode, all its ingress packets are forward in best effort. We recommend that you disable the trusted mode at the ports where the CoS/802.1p and/or DSCP values in the incoming packets are not trustworthy. Otherwise, it might negatively affect the performance of your network.

Configuring Basic QoS Trust Mode

Use the Global Settings page to set the trust behavior for QoS basic mode. This configuration is active when the switch is in QoS basic mode. Packets entering a QoS domain are classified at the edge of the QoS domain.

To define the trust mode for QoS basic mode:

STEP 1 Click **Quality of Service** > **QoS Basic Mode** > **Global Settings**.

STEP 2 Select the trust mode when the switch is in QoS basic 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 is no VLAN tag on the incoming packet), the actual mapping of the VPT to queue can be configured on the 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 on the DSCP to Queue page. If traffic is not IP traffic, it is mapped to the best effort queue.
- **IP Precedence**—Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence to Queue page.
- **CoS/802.1p-DSCP**—Uses the trust CoS mode for non-IP traffic and trust DSCP mode for IP traffic.

STEP 3 Click **Apply**. The Running Configuration is updated.

Configuring Basic QoS Interface Settings

Use the Interface Settings page to configure QoS on each port, as follows:

- **QoS State Disabled**—All inbound traffic on the port is mapped to the best effort queue and no classification/prioritization takes place.
- **QoS State 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 enable or disable QoS on an interface:

STEP 1 Click **Quality of Service** > **QoS Basic Mode** > **Interface Settings**.

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

STEP 3 To enable or disable QoS on an interface, select the desired interface and click **Edit**.

STEP 4 Enter the following information:

- **Interface**—Select the port or LAG to be defined.
- **QoS State**—Check **Enable** to enable QoS on this interface, or uncheck to disable QoS on this interface.

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

Configuring QoS Advanced Mode

Frames that match an ACL and were permitted entrance are implicitly labeled with the name of the ACL that permitted their entrance. QoS advanced mode actions can then be applied to these flows.

In QoS advanced mode, the switch 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 then 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 is 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.

When configuring the QoS advanced mode, note the following:

- An ACL can be configured to one or more class maps regardless of policies.
- A class map can belong to only one policy.
- When a class map using single policer is bound to multiple ports, each port has its own instance of single policer; each applying the QoS on the class map (flow) at a port independent of each other.
- An aggregate policer will apply the QoS to all of its flows in aggregation regardless of policies and ports.

Advanced QoS settings consist of three parts:

- Definition of the rules to match. All frames matching a single group of rules are considered to be a flow.
- Definition of the actions to be applied to frames in each flow that match the rules.
- Binding of the combinations of rules and action to one or more interfaces.

To configure QoS advanced mode, perform the following:

STEP 1 Select the QoS advanced mode for the system on the QoS Properties page, as described in the **Configuring QoS Properties** section.

STEP 2 Select the trust mode for QoS advanced mode on the Global Settings page, as described in the **Configuring Advanced QoS Global Settings** section.

STEP 3 Create ACLs as described in the **Creating ACLs Workflow** section.

STEP 4 If ACLs were defined, create class maps and associate the ACLs with them on the Class Mapping page, as described in the **Configuring Class Mapping** section.

STEP 5 Create a policy on the Policy Table page, as described in the **Configuring QoS Policies** section.

STEP 6 Associate the policy with one or more class maps on the Policy Class Maps page, as described in the **Configuring Policy Class Maps** section.

STEP 7 You can also specify the QoS, if needed, by assigning a policer to a class map when you associate the class map to the policy.

- **Single Policer**—Create a policy that associates a class map with a single policer on the Policy Class Maps page and the Class Mapping page. Within the policy, define the single policer.
- **Aggregate Policer**—Create a QoS action for each flow that sends all matching frames to the same policer (aggregate policer) on the Aggregate Policer page (See **Configuring Aggregate Policers**). Create a policy that associates a class map with the aggregate policer on the Policy Class Maps page.

STEP 8 Bind the policy to the interfaces on the Policy Binding page, as described in the **Configuring Policy Binding** section.

Configuring Advanced QoS Global Settings

Use the Global Settings page to select the trust mode for QoS advanced mode. Packets entering a QoS domain are classified at the edge of the QoS domain.

To define the trust mode:

STEP 1 Click **Quality of Service** > **QoS Advanced Mode** > **Global Settings**.

STEP 2 Enter the following information:

- **Trust Mode** —Select a trust mode while the switch is in QoS 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. The options are:
  - *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 is no VLAN tag on the incoming packet), the actual mapping of the VPT to queue can be configured on the 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 on the DSCP to Queue page. If traffic is not IP traffic, it is mapped to the best effort queue.
- *IP Precedence*—Traffic is mapped to queues based on the IP precedence. the actual mapping of the IP precedence to queue can be configured on the IP Precedence to Queue page.
- *CoS/802.1p-DSCP*—Select to use Trust CoS mode for non-IP traffic and Trust DSCP mode for IP traffic.

▪ **Default Mode Status**—Select the default trust mode (either trusted or untrusted) for interfaces. This provides basic QoS functionality in QoS advanced mode, so that you can trust CoS/DSCP on advanced QoS by default (without having to create a policy).

In QoS advanced mode, when the Default Mode Status is set to Not Trusted, the default CoS values configured on the interface will be used for prioritizing the traffic arriving on the interface.

If you have a policy on an interface then the default mode is irrelevant, the action is according to the policy configuration and unmatched traffic is dropped.

STEP 3 Click **Apply**. The Running Configuration is updated.

Configuring Class Mapping

A class map defines a traffic flow with ACLs. MAC-based ACL, IPv4-based ACL, and IPv6-based 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 switch. Packets that match the same class map are considered to belong to the same flow.

NOTE Defining class maps does not have any effect on QoS. It is 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 super-group called a policy (see the **Configuring QoS Policies** section).

To define a class map:

STEP 1 Click **Quality of Service** > **QoS Advanced Mode** > **Class Mapping**.

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 following information:

- **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 IPv4-based ACL or IPv6-based ACL in the class map.
  - *MAC*—A packet must match the MAC-based ACL in the class map.
  - *MAC or IP*—A packet must match either the IP-based ACL or the MAC-based ACL in the class map.
- **IP**—Select an IPv4-based ACL or IPv6-based ACL for the class map.
- **MAC**—Select a MAC-based ACL for the class map.
- **Preferred ACL**—Select whether packets are first matched to an IP-based ACL or a MAC-based ACL.

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

QoS Policers

You can measure the rate of traffic that matches a predefined set of rules, and to enforce limits, such as limiting the rate of file-transfer traffic that is allowed on a port.

It can be done by using the ACLs in the class maps to match the desired traffic, and by using 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; each applying the QoS on the class map (flow) at ports that are otherwise independent of each other. A single policer is created on the Policy Class Maps 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 of its flows in aggregation regardless of policies and ports. An aggregate policer is created on 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 cannot 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 or be dropped.

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 on the Aggregate Policer page.

Configuring Aggregate Policers

An aggregate policer applies the QoS to one or more class maps, which equates to one or more flows. An aggregation policer can support class maps from different policies and applies the QoS to all of its flows in aggregation regardless of policies and ports.

To define an aggregate policer:

STEP 1 Click **Quality of Service** > **QoS Advanced Mode** > **Aggregate Policer**.

STEP 2 Click **Add**.

STEP 3 Enter the following information:

- **Aggregate Policer Name**—Enter the name of the aggregate policer.
- **Ingress Committed Information Rate (CIR)**—Enter the maximum bandwidth allowed in bits per second.
- **Exceed Action**—Select the action to be performed on incoming packets that exceed the CIR. Possible values are:
  - *Forward*—Packets exceeding the defined CIR value are forwarded.
  - *Drop*—Packets exceeding the defined CIR value are dropped.

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

Configuring QoS Policies

Use the Policy Table page to define advanced QoS polices. Only those policies that are bound to an interface are active (see the **Configuring Policy Binding** section).

Each policy consists of:

- One or more class maps of ACLs which define the traffic flows in the policy.
- One or more aggregates that apply the QoS to the traffic flows in the policy.

After a policy has been added, class maps can be added on the Policy Class Maps page.

To create an advanced QoS policy:

STEP 1 Click **Quality of Service** > **QoS Advanced Mode** > **Policy Table**.

STEP 2 Click **Add**.

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 is updated.

STEP 5 Click **Policy Class Map Table** to display the Policy Class Maps page.

Configuring 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 and click **Go**. All class maps in that policy are displayed.

STEP 3 Click **Add** to add a new class map.

STEP 4 Enter the following information:

- **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.
- **Action Type**—Select the action regarding the ingress CoS/802.1p and/or DSCP value of all matching packets.
  - *Use default trust mode*—Ignores the ingress CoS/802.1p and/or DSCP value. The matching packets are sent as best effort.
  - *Always Trust*—Always trust the CoS/802.1p and DSCP of the matching packet. If a packet is an IP packet, the switch will put the packet in the egress queue based on its DSCP value and the DSCP to Queue Table. Otherwise, the egress queue of the packet is based on the packet's CoS/802.1p value and the CoS/802.1p to Queue Table.
  - *Set*—Manually set the egress queue for all the matching packets. If this option is selected, select **Queue** and enter the queue number in the **New Value** field.
- **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.
- **Aggregate Policer**—If Police Type is Aggregate, select a previously defined aggregate policer.
- **Ingress Committed Information Rate (CIR)**—If Police Type is Single, enter the CIR in kbps. See the description in the **Configuring Bandwidth** section.

- **Exceed Action**—If Police Type is Single, select the action assigned to incoming packets exceeding the CIR. The options are:
  - *None*—No action.
  - *Drop*—Packets exceeding the defined CIR value are dropped.

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

Configuring Policy Binding

Use the Policy Binding page to bind a policy profile to specific interfaces. When a policy profile is bound to a specific interface, it is active on that interface. Only one policy profile can be configured on a single interface, but a single policy can be bound to more than one interface.

When a policy is bound to an interface, it filters and applies QoS to ingress traffic that belongs to the flows defined in the policy. The policy does not apply to traffic egress to the same interface.

NOTE To edit a policy, it must first be removed (unbound) from all those ports to which it is bound.

To define policy binding:

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

STEP 2 Select an existing policy defined on the Policy Table page and the interface type (Port or LAG), and click **Go**.

STEP 3 Check **Binding** under the interfaces to bind the selected policy to them, uncheck to remove (unbind) the policy from the interface.

STEP 4 Click **Apply**. The QoS policy binding is defined, and the Running Configuration is updated.

STEP 5 To view the policies bound to all interfaces, click **Show Policy Binding Per Port**. The Policy Binding Table displays the policy bound to each interface.

STEP 6 Click **Back** to return to the previous page.

19

SNMP

This chapter describes the Simple Network Management Protocol (SNMP) feature that provides a method for managing network devices.

It includes the following topics:

SNMP Versions and Workflow

The Cisco 220 switch functions as an SNMP agent and supports SNMP v1, v2, and v3. It also reports system events to trap receivers using the traps defined in the Management Information Base (MIB) that it supports.

SNMP v1 and v2

To control access to the system, a list of SNMP communities are defined. Each community consists of a community string and its access privilege. The system responds only to SNMP messages specifying the community that has the correct permissions and correct operations.

SNMP agents maintain a list of variables that are used to manage the switch. These variables are defined in the MIB. The MIB presents the variables controlled by the agent. All MIBs supported by the switch are listed in the **Supported MIBs** section.

NOTE Due to the security vulnerabilities of other versions, we recommend that you use SNMPv3.

SNMP v3

In addition to the functionality provided by SNMPv1 and v2, SNMPv3 applies access control and new trap mechanisms to SNMPv1 and SNMPv2 PDUs. SNMPv3 also defines a User Security Model (USM) that includes:

- **Authentication**—Provides data integrity and data origin authentication.
- **Privacy**—Protects against disclosure message content. Cipher Block-Chaining (CBC) is used for encryption. Either authentication alone is enabled on an SNMP message, or both authentication and privacy are enabled on an SNMP message. However, privacy cannot be enabled without authentication.
- **Timeliness**—Protects against message delay or playback attacks. The SNMP agent compares the incoming message time stamp to the message arrival time.
- **Key Management**—Defines key generation, key updates, and key use. The switch supports SNMP notification filters based on Object IDs (OIDs). OIDs are used by the switch to manage device features.

SNMP Workflow

NOTE For security reasons, SNMP is disabled by default. Before you can manage the switch via SNMP, you must enable the SNMP service on the switch as described in the **Configuring TCP/UDP Services** section.

The following is the recommended series of actions for configuring SNMP:

If you decide to use SNMP v1 or v2:

STEP 1 If desired, define SNMP views on the SNMP > Views page, as described in the **Configuring SNMP Views** section.

STEP 2 Define SNMP groups on the SNMP > Groups page, as described in the **Configuring SNMP Groups** section. The group can be associated with the specified SNMP view.

STEP 3 Define an SNMP community on the SNMP > Community page as described in the **Configuring SNMP Communities** section. The community can be associated with access rights and view in Basic mode or with a group in Advanced mode.

- **Basic mode**—The access rights of a community can configure with Read Only or Read Write. In addition, you can restrict the access to the community to only certain MIB objects by selecting a view (defined on the SNMP > Views page).
- **Advanced Mode**—The access rights of a community are defined by a group (defined on the SNMP > Groups page). You can configure the group with a specific security model. The access rights of a group are Read, Write, and Notify.

STEP 4 Define the notification recipients on the SNMP > Notification Recipients SNMPv1,2 page as described in the **Configuring SNMPv1,2 Notification Recipients** section.

If you decide to use SNMP v3:

STEP 1 Define the SNMP engine on the SNMP > Engine ID page, as described in the **Configuring SNMP Engine ID**. Either create a unique engine ID or use the default engine ID.

STEP 2 Optionally, define SNMP views on the SNMP > Views page as described in the **Configuring SNMP Views** section. This limits the range of OIDs available to an SNMP community or an SNMP group.

STEP 3 Define SNMP groups on the SNMP > Groups page as described in the **Configuring SNMP Groups** section. The group can be associated with the specified SNMP view.

STEP 4 Define SNMP users on the SNMP > Users page as described in the **Managing SNMP Users** section. The SNMP users can be associated with an SNMP group.

STEP 5 Define the notification recipients on the SNMP > Notification Recipients SNMPv3 page as described in the **Configuring SNMPv3 Notification Recipients** section.

Supported MIBs

The following standard MIBs are supported by the Cisco 220 switch:

- RFC1213 MIB-II
- RFC1215 Generic-Traps MIB
- RFC1493 (4188) Bridge MIB
- RFC2618 RADIUS Client MIB
- RFC2674 Bridge MIB Extension
- RFC2737 Entity MIB
- RFC2819 RMON
- RFC2863 The Interface Group MIB
- RFC3164 Syslog MIB
- RFC3621 PoE MIB (only available for PoE models)
- RFC3635 Ethernet-Like MIB
- SNMP-COMMUNITY MIB
- SNMP-MIB
- LLDP-MIB
- LLDP-EXT-MED-MIB
- IEEE802.3 Annex 30C MIB
- CISCO-CDP-MIB
- CISCO-ENVMON-MIB
- CISCO-PORT-SECURITY-MIB
- CISCO-IMAGE-MIB
- CISCO-CONFIG-COPY-MIB

Model Object IDs

The following are the switch model Object IDs (OIDs):

Model	Object ID
SF220-24	1.3.6.1.4.1.9.6.1.84.24.1
SF220-24P	1.3.6.1.4.1.9.6.1.84.24.2
SF220-48	1.3.6.1.4.1.9.6.1.84.48.1
SF220-48	1.3.6.1.4.1.9.6.1.84.48.2
SG220-26	1.3.6.1.4.1.9.6.1.84.26.1
SG220-26P	1.3.6.1.4.1.9.6.1.84.26.2
SG220-50	1.3.6.1.4.1.9.6.1.84.50.1
SG220-50P	1.3.6.1.4.1.9.6.1.84.50.2
SG220-28	1.3.6.1.4.1.9.6.1.84.28.5
SG220-28MP	1.3.6.1.4.1.9.6.1.84.28.3
SG220-52	1.3.6.1.4.1.9.6.1.84.52.5

Configuring SNMP Engine ID

The Engine ID is only 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.

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. The SNMP 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 define the SNMP Engine ID:

STEP 1 Click **SNMP** > **Engine ID**.

STEP 2 In the **Local Engine ID** area, set the local Engine ID:

- **Use Default**—Use the device-generated Engine ID. The default Engine ID is based on the switch 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 switch.
- **User Defined**—Enter the local device Engine ID. The field value is a hexadecimal string (range: 10 to 64). Each byte in the hexadecimal character strings is represented by two hexadecimal digits.

STEP 3 Click **Apply**. The local Engine ID is defined, and the Running Configuration is updated.

STEP 4 The **Remote Engine ID Table** lists all remote SNMP Engine IDs supported by the switch. To add a remote Engine ID, click **Add**.

STEP 5 Enter the following information:

- **Server Definition**—Select whether to specify the Engine ID server by IP address or name.
- **IP Version**—Select either **Version 4** or **Version 6** if the server is identified by IP address.
- **Server IP Address/Name**—Enter the IP address or domain name of the remote server that receives the traps.
- **Engine ID**—Enter the Engine ID.

STEP 6 Click **Apply**. The remote Engine ID is defined, and the Running Configuration is updated.

Configuring SNMP Views

A view is a user-defined label for a collection of MIB tree subtrees. Each subtree ID is defined by the OID of the root of the relevant subtrees. You can either use well known names to specify the root of the desired subtree or enter an OID.

Each subtree is either included or excluded in the view being defined.

Use the Views page to configure the SNMP views. The default views cannot be changed. Views can be attached to groups on the SNMP > Groups page or to a community which employs basic access mode on the SNMP > Communities page.

To define SNMP views:

STEP 1 Click **SNMP** > **Views**.

STEP 2 To add a new SNMP view, click **Add**.

STEP 3 Enter the following information:

- **View Name**—Enter a unique view name.
- **Object ID Subtree**—Select **User Defined** to manually define an OID, or select an existing OID from the list. All descendants of this node will be included or excluded in the view.
- **Include In View**—Check to include the selected MIBs in this view, or uncheck to exclude them.

STEP 4 Click **Apply**. The SNMP view is defined, and the Running Configuration is updated.

Configuring 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 are encrypted. So SNMPv1 and SNMPv2 are not secure.

In SNMPv3, the following security functions can be configured:

- **Authentication**—The switch checks that the SNMP user is an authorized system administrator. This is done for each frame.
- **Privacy**—SNMP frames can carry encrypted data.

In SNMPv3, there are three levels of security:

- No security (No authentication and no privacy)
- Authentication (Authentication and no privacy)
- Authentication and privacy (must be add the group with privacy)

SNMPv3 provides a means of controlling the content that each user can read or write and the notifications that they receive. A group defines read or write privileges and a level of security. It becomes operational when it is associated with an SNMP user or community.

NOTE To associate a nondefault view with a group, first create the view on the SNMP > Views page.

To define SNMP groups:

STEP 1 Click **SNMP** > **Groups**.

STEP 2 To add a new SNMP group, click **Add**.

STEP 3 Enter the following information:

- **Group Name**—Enter the new group name.
- **Security Model**—Select the SNMP version (SNMPv1, SNMPv2, or SNMPv3) attached to the group.

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:

- **Security Level**—Check **Enable** to enable the relative security level attached to the group. SNMPv1 and SNMPv2 support neither authentication nor privacy. If SNMPv3 is selected as the security mode, 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 does not encrypt them, meaning that they can be intercepted and read.
  - *Authentication and Privacy*—Authenticates SNMP messages, and encrypts them if the SNMP message origins are authenticated.
- **View**—Choose a previously defined view for Read, Write, and Notify. Associating a view with the Read, Write, and 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. A read-only view must be selected for an SNMP group.
  - *Write*—Management access is write 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*—Sends only traps with contents that is included in the SNMP view selected for notification. Otherwise, there is no restriction on the contents of the traps. Generally you do not need to select the notify view.

STEP 4 Click **Apply**. The SNMP group is defined, and the Running Configuration is updated.

Managing 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 user has the attributes of its group, having the access privileges configured within the associated view.

Groups enable network managers to assign access rights to a group of users, instead of a single user. A user can only be a member of a single group.

To create an SNMPv3 user, an SNMPv3 group must be available. SNMPv3 group can be defined on the SNMP > Groups page.

To define SNMP users:

STEP 1 Click **SNMP** > **Users**.

STEP 2 To create a new SNMP user and assign SNMP access control privileges to the SNMP user, click **Add**.

STEP 3 Enter the following information:

- **User Name**—Enter a name for the user.
- **Group Name**—Select the SNMP group to which the SNMP user belongs.

  NOTE Users who belong to groups that 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 does not require authentication, then the user cannot configure any authentication. The options are:
  - *None*—No user authentication is used.
  - *MD5*—Uses a MD5 password or key to do the authentication.
  - *SHA*—Uses a Secure Hash Algorithm (SHA) password or key to do the authentication.
- **Authentication Password**—Select **Encrypted** to enter an encrypted authentication password, or select **Plaintext** to enter the authentication password in plaintext format. The password that is used for generating a key by the MD5 or Secure Hash Algorithm (SHA) authentication method.
- **Privacy Method**—Select **None** or **DES** as the privacy method.
- **Privacy Password**—Select **Encrypted** to enter an encrypted privacy password, or select **Plaintext** to enter the privacy password in plaintext format. The password that is used for generating a key by the DES method.

STEP 4 Click **Apply**. The SNMPv3 user is added, and the Running Configuration is updated.

Configuring SNMP Communities

Access rights in SNMPv1 and SNMPv2 are managed by defining communities on the SNMP > Communities page. The community name is a type of shared password between the SNMP management station and the device. It is 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.

Use the Communities page to associate 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 or Read Write. In addition, you can restrict the access to the community to only certain MIB objects by selecting a view.
- **Advanced Mode**—The access rights of a community are defined by a group. You can configure the group with a specific security model. The access rights of a group are Read, Write, and Notify.

To define SNMP communities:

STEP 1 Click **SNMP** > **Communities**.

STEP 2 To add a new SNMP community, click **Add**.

STEP 3 Enter the following information:

- **Community String**—Enter the community name (password) used to authenticate the management station to the device.
- **Basic**—In this mode, there is no connection to any group. You can only choose the community access level (Read Only, Read Write, or System Admin) and, optionally, further qualify it for a specific view. By default, it applies to the entire MIB. If this option 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 cannot be made to the community.

Read Write—Management access is read-write. Changes can be made to the switch configuration, but not to the community.

SNMP Admin—Management access is read-write. Changes can be made to the switch's all configuration, so the read-write view is all.

- *View Name*—Check to select an SNMP view (a collection of MIB subtrees to which access is granted).

- **Advanced**—In this mode, the access rights are determined by SNMP group. Select an existing SNMP group from the drop-down menu for the community.

STEP 4 Click **Apply**. The SNMP community is defined, and the Running Configuration is updated.

Configuring SNMP Notification Recipients

Trap messages are generated to report system events, as defined in RFC 1215. The system can generate traps defined in the MIB that it supports.

Trap receivers (or notification recipients) are network nodes where the trap messages are sent by the switch. A list of notification recipients are defined as the targets of trap messages. A trap receiver entry contains the IP address of the node and the SNMP credentials corresponding to the version that will be included in the trap message. When an event arises that requires a trap message to be sent, it is sent to every node listed in the Notification Recipient Table.

Use the Notification Recipients SNMPv1,2 page and the Notification Recipients SNMPv3 page to configure 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 switch to the SNMP management station indicating that a certain event has occurred, such as a link up/down.

This section describes how to configure SNMP notification recipients and includes the following topics:

- Configuring SNMPv1,2 Notification Recipients
- Configuring SNMPv3 Notification Recipients

Configuring SNMPv1,2 Notification Recipients

To define a recipient in SNMPv1,2:

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

STEP 2 To create an SNMPv1,2 notification recipient, click **Add**.

STEP 3 Enter the following information:

- **Server Definition**—Select whether to define the notification recipient by IP address or name.
- **IP Version**—Select either **Version 4** or **Version 6** if the notification recipient is identified by IP address.
- **Recipient IP Address/Name**—Enter the IP address or hostname of the recipient that 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 that the switch waits before re-sending informs. The default is 15 seconds.
- **Retries**—Enter the number of times that the switch resends an inform request. The default is 3.
- **Community String**—Select the SNMP community for the trap manager.
- **Notification Version**—Select the trap SNMP version. Either SNMPv1 or SNMPv2 may be used, with only a single version enabled at a single time.

STEP 4 Click **Apply**. The SNMPv1,2 notification recipient is defined, and the Running Configuration is updated.

Configuring SNMPv3 Notification Recipients

To define a recipient in SNMPv3:

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

STEP 2 To add an SNMPv3 notification recipient, click **Add**.

STEP 3 Enter the following information:

- **Server Definition**—Select whether to define the notification recipient by IP address or name.
- **IP Version**—Select either **Version 4** or **Version 6** if the notification recipient is identified by IP address.
- **Recipient IP Address/Name**—Enter the IP address or hostname of the notification recipient that 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 that the switch waits before re-sending informs. The default is 15 seconds.
- **Retries**—Enter the number of times that the switch resends an inform request. The default is 3.
- **User Name**—Select the user to whom SNMP notifications are sent. In order to receive notifications, this user must be defined on the Users page, and its Engine ID must be remote.
- **Security Level**—Select how much authentication is applied to the packet. The options are:
  - *No Authentication*—Indicates that the packet is neither authenticated nor encrypted.
  - *Authentication*—Indicates that the packet is authenticated but not encrypted.
  - *Privacy*—Indicates that the packet is both authenticated and encrypted.

NOTE The Security Level here will depend on which User Name was selected. If the User Name was configured as No Authentication, the Security Level will be No Authentication only. However, if the User Name has assigned Authentication and Privacy on the Users page, the security level on this screen can be either No Authentication, or Authentication, or Privacy.

STEP 4 Click **Apply**. The SNMPv3 notification recipient is defined, and the Running Configuration is updated.

A

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the Cisco 220 Series Smart Switches.

Cisco Support Community	www.cisco.com/go/smallbizsupport
Cisco Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Firmware Downloads	www.cisco.com/go/smallbizfirmware Select a link to download firmware for Cisco Products. No login is required.
Cisco Open Source Requests	www.cisco.com/go/smallbiz_opensource_request
Cisco 220 Series Switches	www.cisco.com/go/220switches
Warranty Information	www.cisco.com/go/warranty
Regulatory Compliance and Safety Information	www.cisco.com/en/US/docs/switches/lan/csb_switching_general/rcsi/Switch_ClassA_RCSI.pdf
Cisco Partner Central (Partner Login Required)	www.cisco.com/web/partners/sell/smb