ADMINISTRATION GUIDE

Cisco Small Business

200 Series Smart Switch Administration Guide

Contents

1

Getting Started

This chapter provides an introduction to the user interface, and includes the following topics:

- **Starting the Web-based Switch Configuration Utility**
- **Quick Start Switch Configuration**

Starting the Web-based Switch Configuration Utility

This section describes how to navigate the web-based switch configuration utility.

Browser Restrictions

- If you are using a pop-up blocker, make sure it is disabled.

Browsers have the following restrictions:

- If you are using Internet Explorer 6, you cannot directly use an IPv6 address to access the switch. You can, however, use the DNS (Domain Name System) server to create a domain name that contains the IPv6 address, and then use that domain name in the address bar in place of the IPv6 address.
- If you have multiple IPv6 interfaces on your management station, use the IPv6 global address instead of IPv6 link local address to access the switch from your browser.

Launching the Configuration Utility

To open the user interface:

STEP 1 Open a Web browser.

STEP 2 Enter the IP address of the switch you are configuring in the address bar on the browser, and then press **Enter**. The *Login Page* opens.

NOTE When the switch is using the factory default IP address of 192.168.1.254, its power LED flashes continuously. When the switch is using a DHCP-assigned IP address or an administrator-configured static IP address, the power LED is on solid.

Logging In

Logging In

The default username is **cisco** and the default password is **cisco**. The first time that you log in with the default username and password, you are required to enter a new password.

To log in to the device configuration utility:

STEP 1 Enter the username/password. The password can contain up to 64 ASCII characters. Password-complexity rules are described in the **Setting Password Complexity Rules** section of the **Configuring Security** chapter.

STEP 2 If you are not using English, select the desired language from the *Language* drop-down menu. To add a new language to the switch or update a current one, refer to the *Upgrade/Backup Firmware/Language* section.

STEP 3 If this is the first time that you logged on with the default user ID (**cisco**), and the default password (**cisco**) or your password has expired, the Change Password Page opens. See *Password Expiration* for additional information.

STEP 4 Choose whether to select **Disable Password Complexity Enforcement** or not. For more information on password complexity, see the *Setting Password Complexity Rules* section.

STEP 5 Enter the new username/password and click **Apply**.

When the login attempt is successful, the *Getting Started page* opens.

If you entered an incorrect username or password, an error message is displayed, and the *Login Page* remains displayed. If you are having problems logging in, please see the **Launching the Configuration Utility** section in the Cisco Small Business 200 Series Smart Switch Administration Guide for additional information.

Select **Don't show this page on startup** to prevent the *Getting Started* page from being displayed each time that you log on to the system. If you select this option, the *System Summary* page is opened instead of the *Getting Started* page.

Password Expiration

Password Expiration

The *New Password Page* is displayed:

- The first time you access the switch with the default username **cisco** and password **cisco**. This page forces you to replace the factory default password.
- When the password expires, this page forces you to select a new password.

Logging Out

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 in the **General Administrative Information and Operations** chapter.

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 you made during this session.

A red X icon displayed to the left of the **Save** application link indicates that Running Configuration changes have been made that 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 application link are no longer displayed.

To logout, click **Logout** in 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 system, 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 in 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.

Links on the Getting Started Page

Category	Link Name (on the Page)	Linked Page
Initial Setup	Change Device IP Address	*IPv4 Interface Page*
	Create VLAN	*Create VLAN Page*
	Configure Port Settings	*Port Setting Page*
Switch Status	System Summary	*System Summary Page*
	Port Statistics	*Interface Page*
	RMON Statistics	*Statistics Page*
	View Log	*RAM Memory Page*
Quick Access	Change Device Password	*User Accounts Page*

Links on the Getting Started Page

Category	Link Name (on the Page)	Linked Page
	Upgrade Device Software	*Upgrade/Backup Firmware/ Language*
	Backup Device Configuration	*Download/Backup Configuration/Log Page*
	Configure QoS	*QoS Properties Page*
	Configure Port Mirroring	*Port and VLAN Mirroring Page*

This section describes the features of the web-based switch configuration utility.

Application Header

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

Application Links

Application Link Name	Description
	A red X icon displayed to the left of the **Save** application link indicates that Running Configuration changes have been made that have not yet been saved to the Startup Configuration file. Click **Save** to display the *Copy/Save Configuration Page*. Save the Running Configuration file type 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 file type to the Running Configuration, and sets the switch parameters according to the data in the Running Configuration.
Username	Displays the name of the user logged on to the switch. The default username is **cisco**. (The default password is **cisco**.)
Logout	Click to logout of the web-based switch configuration utility.

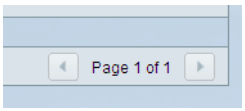
Application Links (Continued)

Application Link Name	Description
About	Click to display the switch name and switch version number.
Help	Click to display the online help.
Language Menu	Select a language or load a new language file into the switch. If the language required is displayed in the menu, select it. If it is not displayed, select **Download Language**. For more information about adding a new language, refer to the *Upgrade/Backup Firmware/Language*.
	The SYSLOG Alert Status icon is displayed 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, follow the **Status and Statistics** > **View Log** > **RAM Memory Page** path.

Management Buttons

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

Management Buttons

Button Name	Description
	Navigate the table by using the right and left arrow icons when there are more than 50 entries in a table.
	Indicates a mandatory field.
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.
Apply	Click to apply 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 changes made on the page.
Clear All Interfaces Counters	Click to clear the statistic counters for all interfaces.
Clear Interface Counters	Click to clear the statistic counters for the selected interface.
Clear Logs	Clears log files.
Clear Table	Clears table entries.
Close	Returns to main page. If there are changes that were not applied to the Running Configuration, a message is displayed.

Management Buttons (Continued)

Button Name	Description
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 it to multiple entries, as described below: 1. Select the entry to be copied. Click **Copy Settings** to display the popup. 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	Select the entry in the table to be deleted and click **Delete** to remove entries from a table. The entry is deleted.
Details	Click to display the details associated with the entry selected on the main page.
Edit	Select the entry and click **Edit** to open the entries for editing. The *Edit* page opens, 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.
Test	Click **Test** to perform the related tests.

2

Viewing Statistics

This chapter describes how to view switch statistics.

It contains the following sections:

- **Viewing Ethernet Interface**
- **Viewing Etherlike Statistics**
- **Viewing 802.1X EAP Statistics**
- **Managing RMON Statistics**

Viewing Ethernet Interface

The *Interface Page* displays traffic statistics per port. 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 display Ethernet statistics:

STEP 1 Click **Status and Statistics** > **Interface**. The *Interface Page* opens.

STEP 2 Enter the parameters.

- **Interface**—Select the type of interface and specific interface for which Ethernet statistics are to be displayed.
- **Refresh Rate**—Select the time period that passes before the interface 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 information 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 information 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.

To clear statistics counters:

- Click **Clear Interface Counters** to clear counters for the interface displayed.
- Click **Clear All Interface Counters** to clear counters for all interfaces.

Viewing Etherlike Statistics

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

To view Etherlike Statistics:

STEP 1 Click **Status and Statistics** > **Etherlike**. The *Etherlike Page* opens.

STEP 2 Enter the parameters.

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

The fields are displayed for the selected interface.

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

To clear statistics counters:

- Click **Clear Interface Counters** to clear the selected interface's Etherlike statistics counters.
- Click **Clear All Interface Counters** to clear the Etherlike statistics counters of all interfaces.

Viewing 802.1X EAP Statistics

The *802.1x EAP Page* displays detailed information regarding the EAP (Extensible Authentication Protocol) frames that were sent or received. To configure the 802.1X feature, see the *802.1X Properties Page*.

To view the EAP Statistics:

STEP 1 Click **Status and Statistics** > **802.1X EAP**. The *802.1x EAP Page* opens.

STEP 2 Select the **Port** that is polled for statistics.

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

The values are displayed for the selected interface.

- **EAPOL Frames Received**—Valid EAPOL frames received on the port.
- **EAPOL Frames Transmitted**—Valid EAPOL frames transmitted by the port.
- **EAPOL Start Frames Received**—EAPOL Start frames received on the port.
- **EAPOL Logoff Frames Received**—EAPOL Logoff frames received on the port.
- **EAP Response/ID Frames Received**—EAP Resp/ID frames received on the port.
- **EAP Response Frames Received**—EAP Response frames received by the port (other than Resp/ID frames).
- **EAP Request/ID Frames Transmitted**—EAP Req/ID frames transmitted by the port.
- **EAP Request Frames Transmitted**—EAP Request frames transmitted by the port.
- **Invalid EAPOL Frames Received**—Unrecognized EAPOL frames received on this port.
- **EAP Length Error Frames Received**—EAPOL frames with an invalid Packet Body Length received on this port.
- **Last EAPOL Frame Version**—Protocol version number attached to the most recently received EAPOL frame.

- **Last EAPOL Frame Source**—Source MAC address attached to the most recently received EAPOL frame.

Managing RMON Statistics

RMON (Remote Networking Monitoring) enables the switch to proactively monitor traffic statistics over a given period and send traps to a remote log server. The switch compares real-time counters against predefined thresholds and generates alarms, without the need for polling by a central management platform. If you have correctly set the thresholds relative to your network's base line, this is an effective management mechanism.

RMON decreases the traffic between the manager and the switch, because the remote log server does not have to frequently poll the switch for information, and it 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 statistics (counter values) as they are currently, meaning since the last time they were cleared.

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
- Rx error event has not been detected
- Packet has a valid CRC

To view the RMON statistics:

STEP 1 Click **RMON** > **Statistics**. The *Statistics Page* opens.

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

STEP 3 Select the **Refresh Rate**, the time period that passes before the interface statistics are refreshed.

The statistics are displayed for the selected interface.

- **Bytes Received (Octets)**—Number of octets received, including bad packets and FCS octets, but excluding framing bits.
- **Drop Events**—Number of packets that were dropped.
- **Packets Received**—Number of packets received, including bad packets, Multicast, and Broadcast packets.
- **Broadcast Packets Received**—Number of good Broadcast packets received. This number does not include Multicast packets.
- **Multicast Packets Received**—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, excluding framing bits, but including FCS octets) received.
- **Jabbers**—Total 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

- **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 65-127 bytes that were received.
- **Frames of 128 to 255 Bytes**—Number of frames, containing 128-255 bytes that were received.
- **Frames of 256 to 511 Bytes**—Number of frames, containing 256-511 bytes that were received.
- **Frames of 512 to 1023 Bytes**—Number of frames, containing 512-1023 bytes that were received.
- **Frames greater than 1024 Bytes**—Number of frames, containing 1024-1632 bytes, and Jumbo Frames, that were received.

STEP 4 Select another interface in the Interface field. The RMON statistics are displayed.

- *Log (Event Log Table)*—Add a log entry to the Event Log table when the alarm goes off.
- *Trap(Syslog Server)*—Send a trap to the remote log server when the alarm goes off.
- *Log and Trap*—Add a log entry to the Event Log table and send a trap to the remote log server when the alarm goes off.

RMON alarms provide a mechanism for setting thresholds and sampling intervals. Exception events can be generated on remote log servers maintained by the agent. Both the rising and falling thresholds must be configured in the alarm. After a rising threshold is crossed, another rising event is not generated until the companion falling threshold is crossed. After a falling alarm is issued, the next alarm is issued when the rising threshold is crossed.

3

Managing 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 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 traps and SYSLOG messages.

This chapter contains the following sections:

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

Setting System Log Settings

You can enable or disable logging on the *Log Settings Page,* and select whether to aggregate log messages.

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

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

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

You can select different severity levels for RAM and Flash logs. These logs are displayed in 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** are stored (Notice, Informational, and Debug).

To set global log parameters:

STEP 1 Click **Administration** > **System Log** > **Logs Settings**. The *Log Settings Page* opens.

STEP 2 Enter the parameters.

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

- **RAM Memory Logging**—Select the severity levels of the messages to be logged to RAM.
- **Flash Memory Logging**—Select the severity levels of the messages to be logged to Flash memory.

STEP 3 Click **Apply**. The switch is updated.

Setting Remote Logging Settings

The *Remote Log Servers Page* enables defining 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 define SYSLOG servers:

STEP 1 Click **Administration** > **System Log** > **Remote Log Servers**. The *Remote Log Servers Page* opens.

This page displays the list of remote log servers.

STEP 2 Click **Add.** The *Add Remote Log Server Page* opens.

STEP 3 Enter the parameters.

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

- **Log Server IP Address/Name** —Enter the IP address or domain name of the log server.
- **UDP Port**—Enter the UDP port to which the log messages are sent.
- **Facility**—Select a facility value from which system logs are sent to the remote server. Only one facility value can be assigned to a server. If a second facility code is assigned, the first facility value is overridden.
- **Description**—Enter a server description.
- **Minimum Severity**—Select the minimum level of system log messages to be sent to the server.

STEP 4 Click **Apply.** The *Add Remote Log Server Page* closes, the SYSLOG server is added, and the switch is updated.

Viewing Memory Logs

The switch can write to the following logs:

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

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

RAM Memory

RAM Memory

The *RAM Memory Page* displays all messages, in chronological order, that were saved in RAM (cache). Entries are stored in the RAM log according to the configuration in the *Log Settings Page*.

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

This page displays the following fields:

- **Log Index**—Log entry number.

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

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

Flash Memory

Flash Memory

The *Flash Memory Page* displays the messages that were stored in Flash memory, in chronological order. The minimum severity for logging is configured in the *Log Settings Page*. Flash logs remain when the switch is rebooted. You can clear the logs manually.

To view the Flash logs click **Status and Statistics** > **View Log** > **Flash Memory**. The *Flash Memory Page* opens.

This page displays the following fields:

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

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

4

Managing System Files

You can choose the firmware file from which the switch boots. You can also copy file types internally on the switch, or to or from an external device, such as a PC.

The methods of file transfer are:

- Internal copy
- HTTP that uses the facilities 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 device. When a configuration is referenced on the switch, it is referenced by its *configuration file type*, as opposed 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 device include firmware, boot code, and log files, and are referred to as *operational files*.

The configuration files are text files and 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.

Files and File Types

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

- **Running Configuration**—Parameters that are currently used by the switch to operate. It is the only file type that is modified by you when the parameter values are changed by using one of the configuration interfaces, and must be manually saved to be preserved.

  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 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 you have made since the last time 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 any time the switch is rebooted. When it is rebooted, 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 a Backup Configuration file. The Backup Configuration exists in Flash and is preserved if the device is rebooted.

- **Mirror Configuration**—A copy of the Startup Configuration, created by the switch after:

  - 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 behaves 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*.

- **Boot Code**—Controls the basic system startup and launches the firmware image.

- **Language File**—The dictionary that allows the windows to be displayed in the selected language.
- **Flash Log**—SYSLOG messages stored in Flash memory.

File Actions

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

- Upgrade the firmware or boot code, or replace a language as described in **Upgrade/Backup Firmware/Language** section.
- Save configuration files on the switch to a location on another device as described in the **Downloading or Backing-up a Configuration or Log** section.
- Clear the Startup Configuration or Backup Configuration file types as described in the **Displaying Configuration File Properties**.
- Copy one configuration file type onto another configuration file type as described in the **Copying Configuration Files**.
- Automatically upload a configuration file from a TFTP server to the switch as described in the **Setting 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.

This chapter describes how configuration and log files are managed.

It includes the following topics:

- **Upgrade/Backup Firmware/Language**
- **Downloading or Backing-up a Configuration or Log**
- **Displaying Configuration File Properties**
- **Copying Configuration Files**
- **Setting DHCP Auto Configuration**

Upgrade/Backup Firmware/Language

The **Upgrade/Backup Firmware/Language** process can be used to:

- Upgrade or backup the firmware image
- Upgrade or backup the boot code
- Import a new language file, upgrade an existing language file, or remove a second language file

The following methods for transferring files are supported:

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

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

The **Upgrade/Backup Firmware/Language** page can also be accessed by selecting **Download New Language** in the Language drop down menu on every page.

A single firmware image is stored on the switch. After uploading a new firmware image to the switch, that image is used. After new firmware has been successfully loaded into the switch, the device needs to be rebooted prior to the new firmware taking effect. The Summary page will continue to show the previous image prior to the reboot.

To download or backup a system or language file:

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

STEP 2 Click the Transfer Method. If you selected TFTP, go to **STEP 3**. If you selected HTTP, go to **STEP 4**.

STEP 3 If you selected TFTP, enter the parameters as described in this step. Otherwise, skip to **STEP 4**.

Select the **Save Action**.

If for the **Save Action** you select *Upgrade* to specify that the file type on the switch is to be replaced with a new version of that file type located on a TFTP server, do the following. Otherwise, go to the next procedure in this step.

a. **File Type**—Select the destination file type. Only valid file types are shown. (The file types are described in the **Files and File Types** section.)

b. **Server Definition**—Select whether to specify the TFTP server by IP address or domain name.

c. **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are:

- *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
- *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.

d. **Link Local Interface**—Select the link local interface (if IPv6 is used) from the list.

e. **TFTP Server IP Address/Name**—Enter the IP address or the domain name of the TFTP server.

f. **Source File Name**—Enter the name of the source file.

If for the **Save Action** you selected *Backup* to specify that a copy of the file type is to be saved to a file on another device, do the following:

a. **File Type**—Select the source file type. Only valid file types can be selected. (The file types are described in the **Files and File Types** section.)

b. **Server Definition**—Select either By IP Address or By name.

c. **IP Version**—Select whether an IPv4 or an IPv6 address is used.

d. **IPv6 Address Type**—Select the IPv6 address type (if used). The options are:

- *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
- *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.

e. **Link-Local Interface**—Select the link local interface (if IPv6 is used) from the list.

f. **TFTP Server IP Address/Name**—Enter the IP address of the TFTP server.

g. **Destination File Name**—Enter the destination file name. File names cannot contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the file name should be between 1 and 160 characters. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_").

STEP 4 If you selected **HTTP**, enter the parameters as described in this step.

Select the **Save Action**—Only supported actions can be selected.

If for the **Save Action** you selected **Upgrade** to specify that the file type on the switch is to be replaced with a new version of that file type, do the following. Otherwise if you selected **Backup**, go to the next procedure in this step.

a. **File Type**—Select the configuration file type. Only valid file types can be selected. (The file types are described in the **Files and File Types** section.)

b. **File Name**—Click *Browse* to select a file or enter the path and source file name to be used in the transfer.

c. Click **Apply**. The file is upgraded.

If for the **Save Action** you selected **Backup** to specify that a copy of the file type is to be saved to a file on another device, do the following:

a. **Source File Type**—Select the configuration file type. Only valid file types are displayed. (The file types are described in the **Files and File Types** section.)

b. Click **Apply**. The **File Download** window displays.

c. Click **Save**. The **Save As** window displays.

d. Click **Save**.

STEP 5 Click **Apply** or **Done**. The file is upgraded or backed up.

Language Files

You can also remove a second language file from the switch if you have two different ones installed. When you open the language menu, you will see the option Delete Language.

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

STEP 2 Click **Delete Language**.

STEP 3 A confirmation window appears asking you to click OK to remove the file.

STEP 4 Click OK to remove the file.

If you already have a second language file and want to load another, you will receive a confirmation window asking you to click OK if you want to replace the existing language file with a new one.

Downloading or Backing-up a Configuration or Log

The *Download/Backup Configuration/Log Page* enables the backup from configuration file types or the flash log on the switch to a file on another device or the restoration of configuration file types from another device to the switch.

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

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

When restoring to Startup Configuration, the switch must be rebooted for the restored Startup Configuration to be used as the Running Configuration. You can reboot the switch by using the process described in the **Rebooting the Switch** section.

To backup or restore the system configuration file:

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

STEP 2 Click the Transfer Method.

STEP 3 If you selected TFTP, enter the parameters. Otherwise, skip to **STEP 4**.

Select the **Save Action**.

If the **Save Action** you selected is *Download* to specify that the file on another device will replace a file type on the switch, do the following. Otherwise, go to the next procedure in this step.

a. **Server Definition**—Select whether to specify the TFTP server by IP address or by domain name.

b. **IP Version**—Select whether an IPv4 or an IPv6 address is used.

NOTE If the server is selected by name in the Server Definition, there is no need to select the IP Version related options.

c. **IPv6 Address Type**—Select the IPv6 address type (if used). The options are:

- *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
- *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.

d. **Link-Local Interface**—Select the link local interface from the list.

e. **Source File Name**—Enter the source file name. File names cannot contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the file name should be between 1 and 160 characters. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_").

f. **Destination File Type**—Enter the destination configuration file type. Only valid file types are displayed. (The file types are described in the **Files and File Types** section.)

If for the **Save Action** you selected *Backup* to specify that a file type is to be copied to a file on another device, do the following:

a. **Server Definition**—Select whether to specify the TFTP server by IP address or by domain name.

b. **IP Version**—Select whether an IPv4 or an IPv6 address is used.

c. **IPv6 Address Type**—Select the IPv6 address type (if used). The options are:

- *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
- *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.

d. **Link-Local Interface**—Select the link local interface from the list.

e. **TFTP Server IP Address/Name**—Enter the IP address or domain name of the TFTP server.

f. **Source File Type**—Enter the source configuration file type. Only valid file types are displayed. (The file types are described in the **Files and File Types** section.)

g. **Destination File Name**—Enter the destination file name. File names cannot contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the file name should be between 1 and 160 characters. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_").

STEP 4 If you selected HTTP, enter the parameters as described in this step.

Select the **Save Action**.

If for the **Save Action** you select *Download* to specify that the file type on the switch is to be replaced with a new version of that file type from a file on another device, do the following. Otherwise, go to the next procedure in this step.

a. **Source File Name**—Click *Browse* to select a file or enter the path and source file name to be used in the transfer.

b. **Destination File Type**—Select the configuration file type. Only valid file types are displayed. (The file types are described in the **Files and File Types** section.)

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

If for the **Save Action** you selected *Backup* to specify that a file type is to be copied to a file on another device, do the following:

a. **Source File Type**—Select the configuration file type. Only valid file types are displayed. (The file types are described in the **Files and File Types** section.)

b. Click **Apply**. The **File Download** window displays.

c. Click **Save**. The **Save As** window displays.

d. Click **Save**.

STEP 5 Click **Apply** or **Done**. The file is upgraded or backed up on the switch (depending upon the file type).

Displaying Configuration File Properties

This *Configuration Files Properties Page* enables the viewing of system configuration file types and the date and time they were modified. It also enables deleting the Startup Configuration and/or the Backup Configuration. You cannot delete the other configuration file types.

To view configuration file properties, click **Administration** > **File Management** > **Configuration Files Properties**. The *Configuration Files Properties Page* opens.

This page provides the following fields:

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

To clear a configuration file, select it and click **Clear Files**.

Copying 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.

The *Copy/Save Configuration Page* enables copying or saving one configuration file to another for backup purposes.

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

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

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

STEP 2 Select the **Source File Name** to be copied. Only valid file types are displayed. (The file types are described in the **Files and File Types** section.)

STEP 3 Select the **Destination File Name** to be overwritten by the source file.

STEP 4 Click **Apply**. The file is copied and switch is updated.

Setting DHCP Auto Configuration

Dynamic Host Configuration Protocol (DHCP) provides a means of passing configuration information (including the IP address of a TFTP server and a configuration file name) to hosts on a TCP/IP network. By default, the switch is enabled as a DHCP client.

When the IP address is allocated or renewed, such as during a reboot or upon an explicit DHCP renewal request and if the switch and the server are configured to do so, the switch transfers a configuration file from the TFTP server identified to the switch by DHCP. This process is known as *auto configuration*.

NOTE If you enable DHCP Auto Configuration on a switch with DHCP disabled, you must enable the DHCP by using the procedure is described in the **IP Addressing** section.

The *DHCP Auto Configuration Page* configures the switch to receive DHCP information pointing to a TFTP server for auto configuration purposes or manual configuration of the TFTP server and configuration file in the event that the information is not provided in a DHCP message.

Note the following limitations regarding the DHCP auto-update process:

- A configuration file that is placed on the TFTP server must match the form and format requirements of a 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.
- To make sure the configuration of devices functions as intended and due to allocation of different IP addresses with each DHCP renew cycle, IP addresses must be bound to MAC addresses in the DHCP server table. This ensures that each device has its own reserved IP address and other relevant information.

To configure DHCP server auto configuration:

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

STEP 2 Enter the values.

- **Auto Configuration Via DHCP**—Select this field to enable or disable the automatic transfer of a configuration from a TFTP server to the Startup Configuration on the switch.
- **Server Definition**—Select By IP Address or By name.
- **Backup TFTP Server IP Address/Name**—Enter the IP address or the name of the TFTP server to be used if no TFTP server IP address was specified in the DHCP message.
- **Backup Configuration File**—Enter the path and file name of the file to be used when no configuration file name was specified in the DHCP message.

The window displays the following:

- **Last Auto Configuration TFTP Server IP Address**—Displays the IP address of the TFTP server last used to perform auto configuration.
- **Last Auto Configuration File Name**—Displays the last file name used by the switch in auto configuration.

  The Last Auto Configuration TFTP Server IP Address and the Last Auto Configuration File Name are compared with the information received from a DHCP server in conjunction with receiving a configuration IP address for the switch. In the event that these values do not match, the switch transfers the configuration file from the TFTP server identified by the DHCP server into the Startup Configuration file, and initiates a reboot. If the values match, no action is taken.

STEP 3 Click **Apply**. The DHCP Auto Configuration is updated.

5

System Time

Network time synchronization is critical because every aspect of managing, securing, planning, and debugging a network involves determining when events occur. Time also provides the only frame of reference between all devices on the network. Without synchronized time, accurately correlating log files between these devices is difficult, even impossible.

A few of the specific reasons include, tracking security breaches, network usage. Problems affecting a large number of components can be nearly impossible to track if timestamps in logs are inaccurate.

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 filesystems reside.

For these reasons, it is important that the time configured on the all devices on the network be accurate.

NOTE The switch supports Simple Network Time Protocol (SNTP) and when enabled, the switch dynamically synchronizes the switch 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 the options for configuring system time, time zone, and Daylight Savings Time (DST). It includes the following topics:

- **System Time Options**
- **Configuring System Time**
- **Adding an SNTP Server**
- **Defining SNTP Authentication**

System Time Options

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

As part of the boot process, the switch always configures the time, time-zone, and DST in some way, either from DHCP, from SNTP, from values set manually, or if all else fails from the factory defaults.

Time

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

- SNTP that 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.

- Manual entry of the system time by the user.
- Entry of the time by the computer that accesses the switch through the device configuration utility. If this feature is enabled, the switch uses the system time from the configuring computer, unless the time has been configured on the switch manually by the user or SNTP server support is not available or enabled.

  NOTE Receiving the time from the computer configuring the switch should be the last resort, such as after a power outage and no other time source is available.

Time Zone and Daylight Savings Time (DST)

The Time Zone and DST can be set on the switch in the following ways:

- Dynamic configuration of the switch through a DHCP server, where:
  - Dynamic DST, when enabled and available, always takes precedence over the manual configuration of DST.
  - If the server supplying the source parameters fails or dynamic configuration is disabled by the user, the manual settings are used.
  - Dynamic configuration of the time zone and DST continues after the IP address lease time has expired.

- Manual configuration of the time zone and DST by the user, where the time zone and DST set manually becomes the Operational time zone and DST, only if the dynamic configuration of the time zone and DST is disabled or fails.

Configuring System Time

Use the *System Time Page* to configure the current time, time zone, DST, and the time source. If the time is determined manually, enter the manual time here.

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 *System Time Page* opens.

STEP 2 Enter the parameters.

- **Clock Source**—Select the source used to set the system clock.
  - **Use Local Settings**—The system time is either entered manually or taken from the configuring computer. If this radio button is selected, enter the Local Settings.
  - **Use SNTP Server**—The system time is obtained from an SNTP server. Also, add an SNTP server and enable SNTP broadcast mode by using the *SNTP Settings Page*. Enforce authentication of the SNTP sessions by using the *SNTP Authentication Page*.
- **Alternate Clock Source**—Select to set the date and time from this computer when Use Local Settings is selected.
- **Get time zone from DHCP**—Select to enable dynamic configuration of the time zone and the DST from the DHCP server. Whether one or both of these parameters can be configured depends on the information found in the DHCP packet. If this option is enabled, *you must also enable DHCP client on the switch*. To do this, set the **IP Address Type** to **Dynamic** in the *IPv4 Interface Page*.

Local Settings—The local time is used when there is no alternate source of time, such as an SNTP server:

- **Date**—Enter the system date.
- **Local Time**—Enter the system time.
- **Time Zone Offset**—Select the difference in hours between *Greenwich Mean Time* (GMT) and the local time. For example, the Time Zone Offset for Paris is GMT +1, while the Time Zone Offset for New York is GMT – 5.
- **Daylight Savings**—Select Daylight Savings to enable DST.
- **Time Set Offset**—Enter the number of minutes that Daylight Savings Time causes clocks to adjust.
- **Daylight Savings Type**—Select how DST is defined:
  - **USA**—According to the dates used in the USA
  - **European**—According to the dates used by the European Union and other countries that use this standard.
  - **By Dates**—Manually, typically for a country other than the USA or a European country. Enter the following parameters:
    - **From**—Day and time that DST starts.
    - **To**—Day and time that DST ends.
    - **Recurring**—DST occurs on the same date every year. Enter the following parameters:

      From—Date when DST begins each year.

      Day—Day of the week on which DST begins every year.

      Week—Week within the month from which DST begins every year.

      Month—Month of the year in which DST begins every year.

      Time—The time at which DST begins every year.

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

      Day—Day of the week on which DST ends every year.

      Week—Week within the month from which DST ends every year.

      Month—Month of the year in which DST ends every year.

Time—The time at which DST ends every year.

STEP 3 Click **Apply**. The system time values are defined, and the switch is updated.

The time settings are displayed in the *Actual Time Details* block.

Adding an SNTP Server

A switch can be configured to synchronize its system clock with an SNTP server by using the *SNTP Settings Page*.

NOTE If specifying an SNTP server by name, this feature requires that the DNS servers be configured on the switch (see the **Defining DNS Servers** section) to work properly.

The switch supports the following modes:

- Broadcast—The SNTP server broadcasts the time, and the switch listens to these broadcasts. When the switch is in this mode, there is no need to define a Unicast SNTP server.
- Unicast SNTP Server Mode—The switch sends Unicast queries to the list of manually-configured SNTP servers, and waits for a response.

The switch supports having both modes active at the same time, choosing the best source of the parameters according to the closest stratum (distance from the reference clock.).

To add an SNTP server:

STEP 1 Click **Administration** > **Time Settings** > **SNTP Settings**. The *SNTP Settings Page* opens.

This page displays the following information for each Unicast SNTP server:

- **SNTP Server**—SNTP server IP address. Up to eight SNTP servers can be defined. The preferred server, or hostname, is chosen according to its stratum level.
- **Poll Interval**—Interval (in seconds) at which the SNTP server is polled for system time information. The poll interval is 1024 seconds.
- **Authentication Key ID**—Key Identification used to communicate between the SNTP server and switch.

- **Preference**—Priority of use for the SNTP server.
  - *Primary*—Server with the lowest stratum level. Stratum level is the distance from the reference clock. Time information is taken from this server.
  - *Secondary*—Server with the next lowest stratum level after the primary server. Serves as a backup to the primary server.
  - *In progress*—SNTP server that is currently sending or receiving SNTP information.
- **Status**—SNTP server status. The possible options are:
  - *Up*—SNTP server is currently operating normally.
  - *Down*—SNTP server is currently not available.
  - *Unknown*—SNTP server is currently being searched for by the switch.
- **Last Response**—Date and time of the last time a response was received from this SNTP server.
- **Offset**—The estimated offset of the server's clock relative to the local clock, in milliseconds. The host determines the value of this offset using the algorithm described in RFC 2030.
- **Delay**—The estimated round-trip delay of the server's clock relative to the local clock over the network path between them, in milliseconds. The host determines the value of this delay using the algorithm described in RFC 2030.

STEP 2 Click **Add** to display the *Add SNTP Server Page*.

STEP 3 Enter the following parameters:

- **Server Definition**—Select if the SNTP server is going to be identified by its IP address or if you are going to chose a well-known SNTP server by name from the list.

  NOTE To specify a well-known SNTP server, the switch must be connected to the Internet and configured with a DNS server or configured so that a DNS server is identified by using DHCP. (See the **Defining DNS Servers** section.)
- **IP Version**—Select the version of the IP address: **Version 6** or **Version 4**.

- **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are
  - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- **Link Local Interface**—Select the link local interface (if IPv6 Address Type Link Local is selected) from the list.
- **SNTP Server IP Address**—Enter the SNTP server IP address. The format depends on which address type was selected.
- **SNTP Server**—Select the name of the SNTP server from a list of well-known SNTP servers. If **other** is chosen, enter the hostname of SNTP server in the adjacent field.
- **Poll Interval**—Select to enable polling of the SNTP server for system time information. All SNTP servers that are registered for polling are polled, and the clock is selected from the server with the lowest stratum level (distance from the reference clock.) that is reachable. The server with the lowest stratum is considered to be the primary server. The server with the next lowest stratum is a secondary server, and so forth. If the primary server is down, the switch polls all servers with the polling setting enabled, and selects a new primary server with the lowest stratum.
- **Authentication**—Select the check box to enable authentication.
- **Authentication Key ID**—If authentication is enabled, select the value of the key ID. (Create the authentication keys using the *SNTP Authentication Page*.)

STEP 4 Click **Apply**. The SNTP server is added, and you are returned to the main page.

Defining SNTP Authentication

The *SNTP Authentication Page* enables configuration of the authentication keys that are used when communicating with an SNTP server that requires authentication.

After a key has been created, it must be bound to one or more relevant SNTP servers to be authenticated. This authentication key can also be used for authentication when receiving Broadcast synchronization.

SNTP sessions might require authentication. A Unicast SNTP server that requires authentication must be bounded with an authentication key when it is added by using the *Add SNTP Server Page*.

To define SNTP authentication:

STEP 1 Click **Administration** > **Time Settings** > **SNTP Authentication**. The *SNTP Authentication Page* opens.

STEP 2 Select **SNTP Authentication** to require authentication of an SNTP session between the switch and an SNTP server.

STEP 3 Click **Apply** to update the switch.

STEP 4 Click **Add.** The *Add SNTP Authentication Page* opens.

STEP 5 Enter the following parameters:

- **Authentication Key ID**—Enter the number used to identify this SNTP authentication key internally.
- **Authentication Key**—Enter the key used for authentication (up to eight characters). The SNTP server must send this key for the switch to synchronize to it.
- **Trusted Key**—Select the check box to allow the switch to receive broadcast synchronization information only from a SNTP server by using this authentication key.

STEP 6 Click **Apply**. The SNTP Authentication is defined, and the switch is updated.

6

General Administrative Information and Operations

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

It includes the following topics:

- System Information
- Switch Models
- Rebooting the Switch
- Monitoring the Fan Status and Temperature
- Defining Idle Session Timeout
- Pinging a Host

System Information

The *System Summary Page* provides a graphic view of the switch, and displays switch status, hardware information, firmware version information, general Power-over-Ethernet (PoE) status, and so forth.

Displaying the System Summary

To view system information, click **Status and Statistics** > **System Summary**. The *System Summary Page* opens.

The System Summary page displays system and hardware information.

System information:

- **System Description**—A description of the system.
- **System Location**—Physical location of the switch. Click **Edit** to go the *System Settings Page* to enter this value.
- **System Contact**—Name of a contact person. Click **Edit** to go the *System Settings Page* to enter this value.
- **Host Name**—Name of the switch. Click **Edit** to go the *System Settings Page* to enter this value. By default, the switch 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).
- **System Object ID**—The unique SNMP object ID for this Cisco product.
- **System Uptime**—Time that has elapsed since the last reboot.
- **Current Time**—Current system time.
- **Base MAC Address**—Switch MAC address.
- **Jumbo Frames**—Jumbo frame support status. This support can be enabled or disabled by using the *Port Setting Page*.

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

TCP/UDP Services Status

- **details**—Clicking on details takes you to *Security > TCP/UDP Services*. See **Chapter 16, Configuring Security** for details.

Hardware and firmware version information:

- **Model Description**—Switch model description.
- **Serial Number**—Serial number.
- **PID VID**—Part number and version ID.
- **Firmware Version** —Firmware version number of the software image.
- **Firmware MD5 Checksum** —MD5 checksum of the software image.
- **Boot Version**—Boot version number.
- **Boot MD5 Checksum**—MD5 checksum of the boot version.
- **Locale**—Locale of the first language. (This is always English.)

- **Language Version**—Firmware version of the primary language of the active image.
- **Language MD5 Checksum**—MD5 checksum of the language file.
- **Locale**—Locale of the second language.
- **Language Version**—Firmware version of the secondary language package.
- **Language MD5 Checksum**—MD5 checksum of the secondary language file.

General PoE Status on models with PoE capability:

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

Configuring the System Settings

To enter system settings:

STEP 1 Click **Administration** > **System Settings**. The *System Settings Page* opens.

STEP 2 Modify the system settings.

- **System Description**—Displays a 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 the host name:
  - *Use Default*—The default hostname (System Name) of these switches is: *switch123456*, where 123456 represents the last three bytes of the switch MAC address in hex format.
  - *User Defined*—Enter the hostname. Use only letters, digits, and hyphens. Host names cannot begin or end with a hyphen. No other symbols, punctuation characters, or blank spaces are permitted (as specified in RFC1033, 1034, 1035).

STEP 3 Click **Apply** to set the values in the Running Configuration.

Switch Models

All models can be fully managed through the web-based switch configuration utility.

Smart Switch Models

Model Name	Product ID (PID)	Description	Ports	Power Dedicated to PoE	No. of Ports that Support PoE
SG 200-18	SLM2016T	18-port Gigabit			
SG 200-26	SLM2024T	26-port Gigabit			
SG 200-26P	SLM2024PT	26-port Gigabit PoE		100W	12 ports e1- e6, e13 - e18
SG 200-50	SLM2048T	50-port Gigabit			
SG 200-50P	SLM2048PT	50-port Gigabit PoE		180W	24 ports e1-e12, e25 - e36
SF 200-24	SLM224GT	24-port 10/100			
SF 200-24P	SLM224PT	24-port 10/100 PoE		100W	12 ports e1- e6, e13 - e18
SF 200-48	SLM248GT	48-port 10/100			
SF 200-48P	SLM248PT	48-port 10/100 PoE		180W	24 ports e1- e12, e25 - e36

Rebooting the Switch

Some configuration changes, such as enabling jumbo frame support, require the system to be rebooted before they take effect. However, rebooting the switch deletes 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. For more information on files and file types, see the **Files and File Types** section in the **Managing System Files** chapter.

You can backup the configuration by using Administration > Save/Copy Configuration or click **Save** at the top of the window. You can also upload the configuration from a remote device see the **"Downloading or Backing-up a Configuration or Log"** section in the **Managing System Files** chapter.

To reboot the switch:

STEP 1 Click **Administration** > **Reboot**. The *Reboot Page* opens.

STEP 2 Click one of the Reboot buttons to reboot the switch.

- **Reboot**—Reboots the switch. Since any unsaved information in the Running Configuration s 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.)
- **Reboot to Factory Defaults**—Reboots 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.

CAUTION DHCP Auto Configuration should be disabled (enabled by default), otherwise a configuration file might be loaded from a TFTP server, instead of the factory default settings.

Monitoring the Fan Status and Temperature

The *Health Page* displays switch fan status and temperature on SG 200-50P. The SG 200-26P, SG 200-50, SF 200-24P, and SF 200-48P devices display only fan status.

To view the switch health parameters, click **Status and Statistics** > **Health**. The *Health Page* opens.

The Health page displays the following fields:

- **Fan Status**—Fan status.
- **Temperature**—Switch temperature.

Defining Idle Session Timeout

The *Idle Session Timeout* configures the time interval during which the HTTP session can remain idle before it times out and the user must login again to reestablish the session.

- **HTTP Session Timeout**

To set the idle session timeout of an HTTP session:

STEP 1 Click **Administration** > **Idle Session Timeout**. The *Idle Session Timeout* page opens.

STEP 2 Select the timeout for the session from the corresponding list. The default timeouts are 10 minutes.

STEP 3 Click **Apply** to set the configuration settings on the switch.

Pinging 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 host:

STEP 1 Click **Administration > Ping**. The *Ping* page opens.

STEP 2 Configure ping by entering the fields:

- **Host Definition**—Select whether to specify hosts by their IP address or name.
- **IP Version**—If the host is identified by its IP address, select either IPv4 or IPv6, to indicate that it will be entered in the selected format.
- **IPv6 Address Type**—Select Link Local or Global as the type of IPv6 address to enter.
  - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- **Link Local Interface**—If the IPv6 address type is Link Local, select from where it is received.
- **Host IP Address/Name**—Address or host name of the device to be pinged. Whether this is an IP address or host name depends on the Host Definition.
- **Ping Interval**—Length of time the system waits between ping packets. Ping is repeated a “Number of Pings” number of times, whether it succeeds or not.
- **Number of Pings** —The number of times the ping operation will be performed.

- **Status**—Displays whether the ping succeeded or failed.

STEP 3 **Click Activate Ping** to ping the host. The ping status is displayed and another message is added to the list of messages, indicating the result of the ping operation.

STEP 4 View the results of ping in the Ping Counters and Status section of the page.

7

Configuring Discovery

This chapter provides information for configuring Discovery.

It includes the following topics:

- **Configuring Bonjour Discovery**
- **Configuring LLDP**

Configuring Bonjour Discovery

As a Bonjour client, the switch periodically broadcasts Bonjour Discovery protocol packets to directly-connected IP subnet(s), advertising its existence and the services that it provides. The switch can be *discovered* by a network management system or other third-party applications. By default, Bonjour is enabled and runs on the Management VLAN. The Bonjour console automatically detects the device and displays it.

Bonjour Discovery can only be enabled globally, and not on a per-port or per-VLAN basis. The switch advertises the services enabled by the administrator.

When Bonjour Discovery and IGMP are both enabled, the IP Multicast address of Bonjour is displayed on the *IP Multicast Group Address Page*.

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

To globally enable Bonjour:

STEP 1 Click **Administration** > **Discovery - Bonjour**. The *Discovery - Bonjour Page* opens.

STEP 2 Select **Enable** to enable Bonjour Discovery globally on the switch.

STEP 3 Click **Apply**. Bonjour is enabled or disabled on the switch according to the selection.

Configuring LLDP

The Link Layer Discovery Protocol (LLDP) enables network managers to troubleshoot and enhance network management by discovering and maintaining network topologies over multi-vendor environments. LLDP discovers network neighbors by standardizing 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.

The LLDP protocol operates by broadcasting Multicast frames from each port. These are referred to as Protocol Data Units (PDUs or LLDP PDUs), and are processed by devices that are aware of the LLDP protocol. The LLDP PDUs pack information in TLVs (type-length-value tuples). The types of TLVs to be broadcast can be configured.

The LLDP protocol has an extension called LLDP Media Endpoint Discovery (LLDP-MED), which provides and accepts information from voice or video devices. For further information about LLDP-MED, see the *LLDP MED Protocol* section.

LLDP Configuration Workflow

Following are examples of actions that can be performed with the LLDP feature:

1. Enable LLDP globally (LLDP is enabled by default), and enter LLDP global parameters, such as the time interval for sending LLDP updates using the *LLDP Properties Page*.
2. Configure LLDP per interface by using the *Port Settings Page*.
3. Create LLDP MED network policies by using the *LLDP MED Network Policy Page*.
4. Associate LLDP MED network policies to ports by using the *LLDP MED Port Settings Page*.
5. View LLDP local port status details by using the *LLDP Local Information Page.*

6. View the LLDP information that was discovered from neighbors, such as local port, system name, time to live, system description, system capabilities by using the *LLDP Neighbors Information Page*.
7. View LLDP-related statistical information per interface by using the *LLDP Statistics Page*.
8. Display overloading information by using the *LLDP Overloading Page*.

Setting LLDP Properties

The *LLDP Properties Page* enables entering LLDP general parameters. These include enabling/disabling the feature globally and setting timers.

To enter LLDP properties:

STEP 1 Click **Administration** > **Discovery - LLDP** > **Properties**. The *LLDP Properties Page* opens.

STEP 2 Enter the parameters.

- **LLDP Status**—Select to enable LLDP on the switch.
- **LLDP PDU Action** —If LLDP is not enabled, select the action to be taken if a packet that matches the selected criteria is received:
  - Discard—Delete the packet.
  - Bridge—Forward the packet to all VLAN members.
- **TLV Advertise Interval**—Enter the rate in seconds at which LLDP advertisement updates are sent.
- **Topology Change System Log Notification Interval**—Enter the minimum time interval between system log notifications.
- **Hold Multiplier**—Enter the amount of time that LLDP packets are held before the packets are discarded, measured in multiples of the TLV Advertise Interval. For example, if the TLV Advertise Interval is 30 seconds, and the Hold Multiplier is 4, then the LLDP packets are discarded after 120 seconds.
- **Reinitializing Delay**—Enter the time interval in seconds that passes between disabling and reinitializing LLDP, following an LLDP enable/disable cycle.
- **Transmit Delay**—Enter the amount of time in seconds that passes between successive LLDP frame transmissions due to changes in the LLDP local systems MIB.

For a description of LLDP MED, refer to the *LLDP MED Protocol* section.

STEP 3 In the **Fast Start Repeat Count** field, enter the number of times LLDP packets are sent when the LLDP-MED Fast Start mechanism is initialized. This occurs when a new endpoint device links to the switch.

STEP 4 Click **Apply**. The LLDP properties are defined.

Editing LLDP Port Settings

Use the *Port Settings Page* to activate LLDP and remote log server notification per port, and to select the TLVs included in LLDP PDUs.

By setting these properties it is possible to select the types of information to be provided to devices that support the LLDP protocol.

The LLDP-MED TLVs to be advertised can be selected in the *LLDP MED Port Settings Page*.

To define the LLDP port settings:

STEP 1 Click **Administration** > **Discovery - LLDP** > **Port Settings**. The *Port Settings Page* opens.

This page displays the port LLDP information.

STEP 2 Select a port and click **Edit.** The *Edit LLDP Port Settings Page* opens.

This page provides the following fields:

- **Interface**—Select the port to be defined.
- **Administrative Status**—Select the LLDP publishing option for the port. The values are:
  - *Tx Only*—Publishes only but does not discover.
  - *Rx Only*—Discovers but does not publish.
  - *Tx & Rx*—Publishes and discovers.
  - *Disable*—Indicates that LLDP is disabled on the port.

- **System Log Notification**—Select **Enable** to notify notification recipients that there has been a topology change.

  The time interval between notifications is entered in the Topology Change System Log Notification Interval field in the *LLDP Properties Page*.

- **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/software version.
  - *System Name*—System's assigned name (in alpha-numeric format). The value equals the sysName object.
  - *System Description*—Description of the network entity (in alpha-numeric 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*—Maximum frame size capability of the MAC/PHY implementation.

The following fields relate to the Management Address:

- **Advertisement Mode**—Select one of the following ways to advertise the IP management address of the switch:
  - *Auto Advertise*—Send the current management IP address of the switch, regardless of whether it was acquired via DHCP or manually.
  - *None*—Do not advertise the management IP address.
  - *Manual Advertise*—Select this option and the management IP address to be advertised.
- **IP Address**—If Manual Advertise was selected, select the Management IP address from the addresses provided.

STEP 3 Enter the relevant information, and click **Apply**. The port settings are modified, and the switch is updated.

LLDP MED Protocol

LLDP Media Endpoint Discovery (LLDP-MED) is an enhancement of LLDP that provides additional capabilities to support media devices.

LLDP-MED:

- Provides detailed network topology information, including the devices located on the network and their location, for example, which IP phone is connected to which port, which software is running on which switch, and which port is connected to which PC.
- 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.
- Provides troubleshooting information. LLDP MED sends alerts to network managers:
  - Port speed and duplex mode conflicts
  - QoS policy misconfigurations

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

Setting LLDP MED Network Policy

An LLDP-MED network policy is a related set of configuration settings identified by a network policy number. This set is loaded into an LLDP-MED TLV, and sent to devices connected to the switch. This information is used by the connected device to send traffic, as specified in the network policy. For example, a policy can be created for VoIP phones that instructs them to:

- Send voice traffic on VLAN 10
- Tag voice traffic with DSCP=63
- Transmit data-traffic to the switch (from the PC connected to the switch through the VoIP phone) without modification to traffic sent by the PC (typically, Untagged).

Network policies are associated with ports by using the *LLDP MED Port Settings Page*. (An administrator must create the VLANs, and configure memberships in the VLANs based on the specification in the LLDP-MED network policies.)

To define an LLDP MED network policy:

STEP 1 Click **Administration** > **Discovery - LLDP** > **LLDP MED Network Policy.** The *LLDP MED Network Policy Page* opens.

This page displays previously-created network policies.

STEP 2 Click **Add** and the *Add LLDP MED Network Policy Page* opens.

This page enables the definition of new policies.

STEP 3 Enter the values.

- **Network Policy Number**—Select the number of the policy to be created.
- **Application**—Select from the list the type of application (type of traffic) 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 they send to the switch.

STEP 4 Click **Apply**. The network policy is defined. Associate the network policy with a port by using the *LLDP MED Port Settings Page*.

Configuring LLDP MED Port Settings

The *LLDP MED Port Settings Page* enables selecting the network policies, configured in the *LLDP MED Network Policy Page,* to be advertised on the port, and selecting 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**. The *LLDP MED Port Settings Page* opens.

This page displays LLDP MED settings, including enabled TLVs, for all ports.

STEP 2 Select a port, and click **Edit.** The *Edit LLDP MED Port Settings Page* opens.

This page enables associating LLDP MED policies to ports.

STEP 3 Enter the parameters.

- **Port**—Select a port to configure. After you have configured this port and clicked **Apply**, you can configure another port without returning to the LLDP MED Port Settings Page.
- **LLDP MED Status**—Enable/disable LLDP MED on this port.

- **System Log Notification**—Select whether the log notification is sent on a per-port basis, when an end station that supports MED has been discovered.
- **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 were created in 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 switch is updated.

Displaying LLDP Port Status

The *LLDP Port Status Table Page* displays the LLDP global information, as well as the LLDP status for every port.

To view the LLDP port status, click **Administration** > **Discovery - LLDP** > **LLDP Port Status**. The *LLDP Port Status Page* opens.

LLDP Port Status Global Information

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

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

LLDP Port Status Table

- **Interface**—Port identifier.
- **LLDP Status**—LLDP publishing option.
- **LLDP MED Status**—Enabled or disabled.
- **Local PoE**—Local PoE information advertised.
- **Remote PoE**—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.

Displaying LLDP Local Information

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

STEP 1 Click **Administration** > **Discovery - LLDP** > **LLDP Local Information**. The *LLDP Local Information Page* opens.

STEP 2 On the bottom of the page, click **LLDP Port Status Table**.

Click **LLDP Local Information Details** to see the details of the LLDP and LLDP-MED TLVs sent to the neighbor.

Click **LLDP Neighbor Information Details** to see the details of the LLDP and LLDP-MED TLVs received from the neighbor.

STEP 3 Select the desired port from the **Port** list.

This page provides the following fields:

Global

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

Management Address

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.
- **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. The possible device classes are:
  - **Endpoint Class 1**—Indicates a generic endpoint class, offering basic LLDP services.

  - **Endpoint Class 2**—Indicates a media endpoint class, offering media streaming capabilities, as well as all Class 1 features.
  - **Endpoint Class 3**—Indicates a communications device class, offering all Class 1 and Class 2 features plus location, 911, Layer 2 switch support, and device information management capabilities.

- **PoE Device Type**—Port PoE type, for example, powered.
- **PoE Power Source**—Port power source.
- **PoE Power Priority**—Port power priority.
- **PoE Power Value**—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

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

- **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.

Displaying LLDP Neighbors Information

The *LLDP Neighbors Information 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** > **Neighbors Information**. The *LLDP Neighbors Information Page* opens.

This page displays the following fields:

- **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 2 Select a local port, and click **Details**. The *Neighbors Information Page* opens.

This page displays the following fields:

Port Details

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

Basic Details

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

Managed Address

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

MAC/PHY Details

- **Auto-Negotiation Supported**—Port speed auto-negotiation support status. The possible values are True and False.

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

802.3 Power via MDI

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

802.3 Details

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

802.3 Link Aggregation

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

MED Details

- **Capabilities Supported**—MED capabilities enabled on the port.
- **Current Capabilities**—MED TLVs advertised by the port.
- **Device Class**—LLDP-MED endpoint device class. The possible device classes are:
  - *Endpoint Class 1*—Indicates a generic endpoint class, offering basic LLDP services.

- *Endpoint Class 2*—Indicates a media endpoint class, offering media streaming capabilities as well as all Class 1 features.
- *Endpoint Class 3*—Indicates a communications device class, offering all Class 1 and Class 2 features plus location, 911, Layer 2 switch support and device information management capabilities.

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

802.1 VLAN and Protocol

- **PVID**—Advertised port VLAN ID.

PPVID

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

VLAN IDs

- **VID**—Port and Protocol VLAN ID.
- **VLAN Names**—Advertised VLAN names.

Protocol IDs

- **Protocol ID**—Advertised protocol IDs.

Location Information

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

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

Network Policies

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

Accessing 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 *LLDP Statistics Page* opens.

For each port, the fields are displayed:

- **Interface**—Identifier of interface.
- **Tx Frames Total**—Number of transmitted frames.
- **Rx Frames**
  - **Total**—Number of received frames.
  - **Discarded**—Total number of received frames that were discarded.

- **Errors**—Total number of received frames with errors.

- **Rx TLVs**
  - **Discarded**—Total number of received TLVs that were discarded.
  - **Unrecognized**—Total number of received TLVs that were unrecognized.

- **Neighbor's Information Deletion Count**—Number of neighbor ageouts on the interface.

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

LLDP Overloading

LLDP adds information to packets, and can create oversized packets. The information that LLDP adds is divided into groups. The switch transmits the maximum number of whole groups possible, meaning that no partial groups are transmitted.

The *LLDP Overloading Page* displays the number of bytes sent and number of bytes remaining to be sent for LLDP TLVs per port, and the port's transmission status.

To view LLDP overloading information:

STEP 1 Click **Administration** > **Discovery - LLDP** > **LLDP Overloading**. The *LLDP Overloading Page* opens.

This page displays the following fields for each port:

- **Interface**—Port identifier.
- **Total (Bytes)**—Total number of bytes in each packet.
- **Left to Send (Bytes)**—Total number of bytes left to add into the packet.
- **Status**—Whether TLVs are being transmitted or if they are overloaded.

STEP 2 To view the overloading details for a port, select it and click **Details**. The *LLDP Overloading Details* opens.

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

- **LLDP Mandatory TLVs**

- *Size (Bytes)*—Total mandatory TLV byte size.
- *Status*—If the mandatory TLV group is being transmitted, or if the TLV group was overloaded.

- **LLDP MED Capabilities**
  - *Size (Bytes)*—Total LLDP MED capabilities packets byte size.
  - *Status*—If the LLDP MED capabilities packets were sent, or if they were overloaded.
- **LLDP MED Location**
  - *Size (Bytes)*—Total LLDP MED location packets byte size.
  - *Status*—If the LLDP MED locations packets were sent, or if 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 Extended Power via MDI**
  - *Size (Bytes)*—Total LLDP MED extended power via MDI packets byte size.
  - *Status*—If the LLDP MED extended power via MDI packets were sent, or if they were overloaded.
- **802.3 TLVs**
  - *Size (Bytes)*—Total LLDP MED 802.3 TLVs packets byte size.
  - *Status*—If the LLDP MED 802.3 TLVs packets were sent, or if they were overloaded.
- **LLDP Optional TLVs**
  - *Size (Bytes)*—Total LLDP MED optional TLVs packets byte size.
  - *Status*—If the LLDP MED optional TLVs packets were sent, or if they were overloaded.

- **LLDP MED Inventory**
  - *Size (Bytes)*—Total LLDP MED inventory TLVs packets byte size.
  - *Status*—If the LLDP MED inventory packets were sent, or if they were overloaded.
- **Total (Bytes)**—Total number of packets sent (in bytes).
- **Left to Send (Bytes)**—Total number of packet bytes left to transmit.

8

Port Management

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

It contains the following topics:

- **Setting the Basic Port Configuration**
- **Configuring Link Aggregation**
- **Green Ethernet**

Configuring Ports

Port Management Workflow

To configure ports, perform the following actions:

1. Configure port by using the *Port Setting Page*.
2. Enable/disable the Link Aggregation Control protocol, and configure the potential member ports to the desired Link Aggregation Groups (LAGs) by using the *LAG Management Page*. By default, all LAGs have no port members.
3. Configure the Ethernet parameters, such as speed and auto negotiation for the Link Aggregation Groups by using the *LAG Settings Page*.
4. Configure the LACP parameters for the ports that are members or candidates of a Link Aggregation Group by using the *LACP Page.*
5. Configure global Green Ethernet settings by using the *Properties Page*.
6. Configure per port Green Ethernet energy mode by using the *Port Settings Page*.
7. If PoE is supported and enabled for the switch, configure the switch as described in **Managing Power-over-Ethernet Devices**.

Setting the Basic Port Configuration

The *Port Setting Page* displays the global and per port setting of all the ports. This page enables you to select and configure the desired ports from the *Edit Port Setting Page*.

NOTE SFP Fiber takes precedence when both ports are being used.

To configure port settings:

STEP 1 Click **Port Management** > **Port Settings**. The *Port Setting Page* opens.

STEP 2 Select (**Jumbo Frames) Enable** to support packets of up to 10 Kb in size. If **Jumbo Frames** is not enabled, the system supports packet size up to 1,632 bytes.

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

Jumbo frames configuration changes take effect *only* after the Running Configuration is explicitly saved to the Startup Configuration File using the *Copy/Save Configuration Page*, and the switch is rebooted.

STEP 4 To update the port settings, select the desired port, and click **Edit.** The *Edit Port Setting Page* opens.

STEP 5 Modify the following parameters:

- **Port**—Select the port number.
- **Port Description**—Enter the port user-defined name or comment.
- **Port Type**—Displays the port type. The possible options are:
  - *Copper Ports*—Regular, not combo, support the following values: 10M, 100M, 1000M (type: Copper).
  - *Combo Ports Copper*—Combo port connected with copper CAT5 cable, supports the following values: 10M, 100M, 1000M (type: ComboC).
  - *Combo Fiber—SFP Fiber Gigabit Interface Converter Port* with the following values: 100M and 1000M (type: ComboF)
- **Administrative Status**—Select whether the port should be operational (Up) or non-operational (Down) when the switch is rebooted.
- **Operational Status**—Displays the current port connection status.
- **Reactivate Suspended Port**—Select to reactivate a port that has been suspended. There are numerous ways that a port can be suspended, such as through the locked port security option.

- **Auto-Negotiation**—Select 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 speed setting options are available. You can designate *Administrative Speed* only when port auto-negotiation is disabled.
- **Operational Port Speed**—Displays the current port speed that is the result of negotiation.
- **Administrative Duplex Mode**—Select the port duplex mode. This field is configurable only when auto-negotiation is disabled, and the port speed is set to 10M or 100M. 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**—Select the capabilities to be advertised by the port. The options are:
  - *Max Capability*—All port speeds and duplex mode settings can be accepted.
  - *10 Half*—10 Mbps speed and Half Duplex mode.
  - *10 Full*—10 Mbps speed and Full Duplex mode.
  - *100 Half*—100 Mbps speed and Half Duplex mode.
  - *100 Full*—100 Mbps speed and Full Duplex mode.
  - *1000 Full*—1000 Mbps speed and Full Duplex mode.

NOTE To change the status of a Giga port from 10 Half/100 Half to 1000 Full, change the duplex mode to Full and then change the Administrative Port speed to 1000.

- **Operation Advertisement**—Displays the capabilities currently published to the port's neighbor to start the negotiation process. The possible options are those specified in the *Administrative Advertisement* field.
- **Back Pressure**—Select the Back Pressure mode on the port (used with Half Duplex mode) to slow down the packet reception rate when the switch is congested. It disables the remote port, preventing it from sending packets by jamming the medium.
- **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).
- **MDI/MDIX**—the *Media Dependent Interface* (MDI)/*Media Dependent Interface with Crossover* (MDIX) status on the port. The switch ports are wired by following the Telecommunications Industry Association standards.

  The options are:

  - *MDIX*—Select to connect this switch to hubs and switches by using a straight through cable. This switch swaps its transmit and receives pairs, so that this switch can be connected with another switch or a hub by using a straight through cable.
  - *MDI*—Select to connect this switch to a station by using a straight through cable.
  - *Auto*—Select to configure this switch to automatically detect the correct pinouts for the connection to another device. If the other device supports AutoMDX and the parameter is set to Auto, typically the devices negotiate the pinouts, based on the type of cable connecting the devices and the transmit and receive pinout configuration on each port.
- **Operational MDI/MDIX**—Displays the current MDI/MDIX setting.
- **Member in LAG**—Displays the LAG, if the port is a member of a LAG.

STEP 6 Click **Apply**. *The Port Settings* are modified, and the switch is updated.

Configuring another port by selecting the desired port from the Port field at the top of the *Edit Port Setting Page*.

Configuring Link Aggregation

Link Aggregation Control Protocol (LACP) is part of an IEEE specification (802.3ad) 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 (Link Aggregation Control Protocol) is disabled. You configure a static LAG with a group of ports that are always active members of the LAG.
- *Dynamic*—A LAG is dynamic if it is LACP-enabled. You define a group of ports as candidate ports of a dynamic LAG. The LACP determines which candidate ports from the LAG are active member ports. The non-active member ports are *standby* ports ready to replace any failing active member ports.

Load Balancing

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

This traffic balancing is managed by a hash-based distribution function that distributes Unicast and Multicast traffic based on packet header information.

The switch support 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 and source IP addresses for IP packets, and destination and source MAC addresses for non-IP packets.

LAG Management

Active member ports in a LAG are defined statically by explicit user assignment or are dynamically selected by the Link Aggregation Control Protocol (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 four LAGs.

Every LAG has the following characteristics:

- All ports in a LAG must be of the same media type.
- To add a port to the LAG, it cannot belong to any VLAN except the default VLAN.
- Ports in a LAG must not be assigned to another LAG.
- No more than eight ports are assigned to a static LAG and no more than 16 ports can be candidates for a dynamic LAG.
- All the *ports* in a LAG must have auto-negotiation disabled, although the *LAG* can have auto-negotiation enabled.
- When a port is added to the original configuration of the LAG, the configuration that existed for the port is no longer applied, and 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.

Static and Dynamic LAG Workflow

To configure a **static** LAG, perform the following actions:

1. Configure the selected LAG as a static LAG by disabling LACP on the LAG. Assign up to eight active member ports to the static LAG by selecting and moving the ports from the **Port List** to the **LAG Members** list by using the *LAG Management Page*.
2. Configure the LAG speed and flow control by using the *LAG Settings Page*.

To configure a **dynamic** LAG, perform the following actions:

1. Configure the selected LAG as a dynamic LAG by enabling 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 by using the *LAG Management Page*.
2. Configure the LAG speed and flow control by using the *LAG Settings Page*.
3. Configure the LACP parameters of the ports in the LAG by using the *LACP Page*.

Defining LAG Management

The *LAG Management Page* displays the global and per LAG settings. The page also enables you to configure the global setting and to select and edit the desired LAG on the *Edit LAG Membership Page*.

STEP 1 To configure LAG management, click **Port Management** > **Link Aggregation** > **LAG Management.** The *LAG Management Page* opens.

STEP 2 Select one of the following **Load Balance Algorithms**:

- *MAC Address*—Perform loading balancing by source and destination MAC addresses on all packets.
- *IP/MAC Address*—Perform load balancing by the source and destination IP addresses on IP packets, and by the source and destination MAC addresses on non-IP packets

STEP 3 Click **Apply.** The Load Balance Algorithm is defined, and the switch is updated.

Defining Member Ports in a LAG

The LAG Management Page enables you to define the member ports in a LAG.

STEP 1 Select the LAG to be configured, and click **Edit.** The *Edit LAG Membership Page* opens.

STEP 2 Enter the values for the following fields:

- **LAG**—Select the LAG number.
- **LAG Name**—Enter the LAG name or a comment.
- **LACP**—Select to enable LACP on the selected LAG. This makes it a dynamic LAG.
- **Port List**—Move those ports that are to be assigned to the LAG from the **Port List** to the **LAG Members** list. Up to eight ports per static LAG can be assigned, and 16 ports can be assigned to a dynamic LAG.

STEP 3 Click **Apply.** The LAG membership is defined, and the switch is updated.

You can select another LAG for configuration by changing the LAG field.

Configuring LAG Settings

The *LAG Settings Page* displays a table of current settings for all LAGs. You can configure the settings of selected LAGs, and reactivate suspended LAGs by launching the *Edit LAG Settings Page*.

To configure the LAG:

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

STEP 2 Select a LAG, and click **Edit**. The *Edit LAG Settings Page* opens.

STEP 3 Enter the values for the following fields:

- **LAG**—Select the LAG ID number.
- **Description**—Enter the LAG name or a comment.
- **LAG Type**—Displays the port type that comprises the LAG.
- **Administrative Status**—Set the selected LAG to operational (Up) or non-operational (Down).
- **Operational Status**—Displays whether the LAG is currently operating.
- **Reactivate Suspended LAG**—Select to reactivate a port if the LAG has been disabled through the locked port security option.
- **Administrative Auto-Negotiation**—Enables or disable auto-negotiation on the LAG. Auto-negotiation is a protocol between two link partners that enables a LAG to advertise its transmission rate and flow control to its partner (the Flow Control default is *disabled*). It is recommended to keep auto-negotiation enabled on both sides of an aggregate link, or disabled on both sides, while ensuring that link speeds are identical.
- **Operational Auto-Negotiation**—Displays the auto-negotiation setting.
- **Administrative Speed**—Select the LAG speed.
- **Operational LAG Speed**—Displays the current speed at which the LAG is operating.
- **Administrative Advertisement**—Select the capabilities to be advertised by the LAG. The options are:
  - *Max Capability*—All LAG speeds and both duplex modes are available.

  - *10 Full*—The LAG advertises a 10 Mbps speed and the mode is full duplex.
  - *100 Full*—The LAG advertises a 100 Mbps speed and the mode is full duplex.
  - *1000 Full*—The LAG advertises a 1000 Mbps speed and the mode is full duplex.

- **Operational Advertisement**—Displays the Administrative Advertisement status. The LAG advertises its capabilities to its neighbor LAG to start the negotiation process. The possible values are those specified in the *Administrative Advertisement* field.
- **Neighbor Advertisement**—Displays the neighbor LAG (the LAG to which the selected interface is connected) that advertises its capabilities to the LAG to start the negotiation process. The possible values are the same as those listed in the *Administrative Advertisement* field.
- **Administrative Flow Control**—Enable or disable Flow Control or enable the auto-negotiation of Flow Control on the LAG.
- **Operational Flow Control**—Displays the current Flow Control setting.

STEP 4 Click **Apply**. The switch is updated.

You can select another LAG for configuration by changing the LAG field.

Configuring LACP

A dynamic LAG is LACP-enabled; the Link Aggregation Control Protocol is run on every candidate port defined in the LAG.

LACP system priority and LACP port priority determine which of the candidate ports become active member ports in a dynamic LAG configured with more than eight candidate ports. The selected candidate ports of the LAG are all connected to the same remote device.

An LACP channel group 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 an LACP channel-group, the switch on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other switch (the non-controlling end of the link) are ignored.

The LACP priority is taken either from the local or the remote device according to the following rule: The local LACP System Priority is compared to the remote LACP System Priority device. The lowest priority is used. If both priorities are the same, the local and remote MAC addresses are compared. The priority of the device with the lowest MAC address is used.

The additional rules in selecting the active or standby ports in a dynamic LACP are as follows:

- Any link operating at a different speed from the highest-speed active member or operating at half-duplex is made 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 is made inactive, and placed in standby mode.

Setting Port LACP Parameter Settings

The *LACP Page* displays and enables configuration of the LACP System Priority, LACP timeout, and LACP port priority. 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, 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**. The *LACP Page* opens.

STEP 2 Enter the global **LACP System Priority** value that determines which candidate ports will become members of the LAG.

The page displays the LACP settings of every port. You can select and edit the desired port by using the *Edit LACP Page*

STEP 3 Select a port, and click **Edit.** The *Edit LACP Page* opens.

STEP 4 Enter the values for the following fields:

- **Port**—Select the port number to which timeout and priority values are assigned.
- **LACP Port Priority**—Enter the LACP priority value for the port.

- **LACP Timeout**—Select the periodic transmissions of LACP PDUs occur at either a slow or fast transmission rate, depending upon the expressed LACP timeout preference.

STEP 5 Click **Apply**. The switch is updated.

You can continue editing by selecting another port in the Port field.

Green Ethernet

Green Ethernet is a common name for a set of features that are designed to be environmentally friendly, and to reduce the power consumption of a device.

The Green Ethernet feature reduces overall power usage in two ways:

- **Energy-Detect Mode**—On an inactive link, the port moves into inactive mode, saving power while keeping the Administrative status of the port Up. Recovery from this mode to full operational mode is fast, transparent, and no frames are lost. This mode is supported on both GE and FE ports.
- **Short-Reach Mode**—Cable length is analyzed, and the power usage is adjusted for various cable lengths. In this mode, the VCT (Virtual Cable Tester) length test is performed to measure cable length. If the cable is shorter than a predetermined length, the switch uses less power to send frames over the cable, thus saving energy. This mode is only supported on RJ45 GE ports; it does not apply to the GE ports with the Combo Port.

The two Green Ethernet modes: Energy Detect Mode and Short Reach Mode must be enabled globally and configured per port.

Power savings and current power consumption can be monitored. The total amount of saved energy can be viewed as a percentage of the power that would have been consumed by the physical interfaces had they not been running in Green Ethernet mode.

Power savings can be monitored.

The Green Ethernet features are defined per port, regardless of their LAG membership.

Setting Global Green Ethernet Properties

The *Properties Page* displays and enables configuration of the Green Ethernet mode for the switch. It also displays the current power savings.

To define Global Green Ethernet properties:

STEP 1 Click **Port Management** > **Green Ethernet** > **Properties**. The *Properties Page* opens.

STEP 2 Enter the values for the following fields:

- **Energy Detect Mode**—Globally enable or disable Energy Detect mode. If this mode is changed, a message is displayed.

  The Energy mode is changed when you click **OK**.

- **Short Reach Mode**—Globally enable or disable Short Reach mode if there are GE ports on the switch.

  NOTE Disabling or enabling Energy Detect Mode temporarily disconnects the network connections.

- **Power Savings**—Displays the power saved by running in Green Ethernet mode.

- **Cumulative Energy Saved**—Displays the amount of energy saved from the last switch reboot. This value is updated each time there is an event that affects power saving.

STEP 3 Click **Apply**. *The Port Settings* are modified, and the switch is updated.

Setting Green Ethernet Properties for Ports

The *Port Settings Page* displays the current Green Ethernet Energy mode for each port, and enables selecting a port for Green Ethernet Energy configuration by using the *Edit Port Setting Page*. For the Green Ethernet modes to operate on a port, the corresponding modes must be activated globally in the *Properties Page.*

To define per port Green Ethernet settings:

STEP 1 Click **Port Management** > **Green Ethernet**> **Port Settings**. The *Port Settings Page* opens.

The *Port Settings Page* displays the following:

- **Entry number**—The sequential number of the entry in the table.
- **Port**—The port number.
- **Energy Detect**—State of the port regarding Energy Detect mode:
  - *Administrative*—Displays whether Energy Detect mode was enabled.
  - *Operational*—Displays whether Energy Detect mode is currently operating.
  - *Reason*—If Energy Detect mode is not operational, displays the reason.
- **Short Reach**—State of the port regarding Short Reach mode:
  - *Administrative*—Displays whether Short Reach mode was enabled.
  - *Operational*—Displays whether Short Reach mode is currently operating.
  - *Reason*—If Short-Reach mode is not operational, displays the reason.

  NOTE The window displays the Short Reach setting for each port; however, the Short Reach feature is *not enabled* on any port unless the Short Reach feature is also enabled globally by using the *Properties Page*. To enable Short Reach globally, see the **Setting Global Green Ethernet Properties** section.
- **Cable Length**—Displays VCT cable length in meters.

STEP 2 Select a **Port** and click **Edit**. *The Edit Port Setting Page* opens.

STEP 3 Select to enable or disable Energy Detect mode on the port.

STEP 4 Select to enable or disable Short Reach mode on the port.

STEP 5 Click **Apply**. The Green Ethernet port settings are modified, and the switch is updated.

Select another port to display or edit that port.

9

Managing Device Diagnostics

This chapter contains information for configuring port mirroring, running cable tests, and viewing device operational information.

It includes the following topics:

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

Testing Copper Ports

The *Copper Ports Page* displays the results of integrated cable tests performed on copper cables.

Two types of tests are used:

- Time Domain Reflectometry (TDR) technology tests the quality and characteristics of a copper cable attached to a port. Cables of up to 100 meters long can be tested. Cables over 100 meters might not have accurate results.
- DSP-based tests are performed on active GE links to measure length.

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

To test copper cables attached to ports:

STEP 1 Click **Administration** > **Diagnostics** > **Copper Ports**. The *Copper Ports Page* opens.

This page displays the results of previously-conducted basic tests.

STEP 2 To perform a Basic test, select a port from the list of ports, and click **Basic Test**. A message displays indicating that the test causes the link to briefly go down.

STEP 3 Click **OK** to confirm that the link can go down or click **Cancel** to abort the test.

The results are displayed on the page:

- **Test Result**—Cable test results. Possible values are:
  - *OK*—Cable passed the test.
  - *No Cable*—Cable is not connected to the port.
  - *Open Cable*—Cable is connected on only one side.
  - *Short Cable*—Short circuit has occurred in the cable.
  - *Unknown Test Result*—Error has occurred.
- **Distance to Fault**—Distance from the port to the location on the cable where the fault was discovered.
- **Cable Length**—Estimated cable length, available only for 1 GB links, excluding Combo ports.

  NOTE The cable length is **Unknown** when the green features are enabled.

  NOTE The supported length for Ethernet cables is 100M; any size above that is unpredictable.
- **Last Update**—Time of the last test conducted on the port.

STEP 4 To perform the Advanced test on all GE ports, click **Advanced Test.** The *Copper Cable Extended Feature Page* opens.

NOTE To avoid unknown results in the Advanced Test, perform the Basic Test first.

This page displays the results of the most recent test:

- **Port**—Port identifier.
- **Cable Status**—Cable status.

- **Speed**—Link speed.
- **Link Status**—Current link Up/Down status.
- **Pair**—Cable wire pairs being tested.
- **Distance to Fault**—Distance between the port and the location on the cable where the fault was discovered.
- **Status**—Wire pair status. Red indicates fault and Green indicates status OK.
- **Cable length**—Cable length in meters.

  If the link is down, TDR Technology is used to test the GE and FE ports. Cable length measurements are accurate to within 3 to 4 meters.

  If the link is up, DSP Technology is used to test the GE ports. (FE ports are not tested for length.).
- **Channel**—Cable channel.
- **Polarity**—Indicates if automatic polarity detection and correction has been activated for the wire pair.
- **Pair Skew**—Difference in delay between wire pairs.

STEP 5 Click **Close** to close the window.

Displaying Optical Module Status

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

MSA-compatible SFPs

The following FE SFP (100Mbps) 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 (1000Mbps) 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 results of optical tests. click **Administration** > **Diagnostics** > **Optical Module Status**. The *Optical Module Status Page* opens.

This page displays the following fields:

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

- **Output Power**—Transmitted optical power.
- **Input Power**—Received optical power.
- **Transmitter Fault**—Remote SFP reports signal loss. Values are True, False, and No Signal (N/S).
- **Loss of Signal**—Local SFP reports signal loss. Values are True and False.
- **Data Ready**—SFP is operational. Values are True and False

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 switch port. This 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 displays the data packets for diagnosing, debugging, and performance monitoring. Up to eight sources can be mirrored. This can be any combination of eight individual ports and/or VLANs.

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 port(s) is received on the analyzer (destination) port. If more data is sent to the analyzer port than it can support, some data might be lost.

Only one instance of mirroring is supported system-wide. The analyzer port (or target port for VLAN mirroring or port mirroring) is the same for all the mirrored VLANs or mirrored ports.

To enable port and VLAN mirroring:

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

This page displays the following fields:

- **Destination Port**—Port to which traffic is to be copied; the analyzer port.

- **Source Interface**—Interface, port, or VLAN, from which traffic is sent to the analyzer port.
- **Type**—Type of monitoring: incoming to the port, outgoing from the port, or both.
- **Status**—Whether the interface is up or down.

STEP 2 Click **Add** to add a port or VLAN to be mirrored. The *Add Port/VLAN Mirroring Page* opens.

STEP 3 Enter the parameters:

- **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. A port identified as a analyzer destination port, it remains the analyzer destination port until all the entries are removed.
- **Source Interface**—Select Port or VLAN as the source port or source VLAN from where traffic is to be mirrored.
- **Type**—Select whether incoming, outgoing, or both types of traffic are mirrored to the analyzer port. If **Port** is selected, 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.

STEP 4 Click **Apply**. Port mirroring is added, and the switch is updated.

Viewing CPU Utilization

The *CPU Utilization Page* displays the switch CPU utilization. You can enable or disable CPU utilization monitoring, and configure the rate at which the graph is updated.

To enable and display CPU utilization:

STEP 1 Click **Administration** > **Diagnostics** > **CPU Utilization**. The *CPU Utilization Page* opens.

STEP 2 Select **CPU Utilization** to enable viewing CPU resource utilization information.

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

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

10

Managing Power-over-Ethernet Devices

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

This chapter describes how to use the PoE feature.

It includes the following topics:

- **PoE on the Switch**
- **Configuring PoE Properties**
- **Configuring the PoE Power, Priority, and Class**

PoE on the Switch

A PoE switch is PSE (Power Sourcing Equipment) that delivers electrical power to connected PD (Powered Devices) 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.

Power over Ethernet 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 Power Sourcing Equipment (PSE) and the Powered Device (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 PD. If the PD supports PoE, but without classification, it is assumed to be class 0 (the maximum). If a PD tries to consume more power than permitted by the standard, the PSE stops supplying power to the port.

PoE supports two modes:

- Port Limit—The maximum power the switch agrees to supply is limited to the value the system administrator configures, regardless of the Classification result.
- Class Power Limit—The maximum power 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:

- Maximum power a PSE is allowed to supply to a PD
- During device operation, to change the mode from Class Power Limit to Port Limit and vice versa. The power values per port that were configured for the Port Limit mode are retained.
- 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.

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 (Class Limit mode).

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
- Logs the reason for turning off power
- Generates a trap to a remote log server

Configuring PoE Properties

The *PoE Properties Page* enables selecting either the Port Limit or Class Limit PoE mode and specifying the PoE traps to be generated.

These settings are entered in advance. When the PD actually connects and is consuming power, it might consume much less than the maximum power allowed.

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

To configure PoE on the switch and monitor current power usage:

STEP 1 Click **Port Management > PoE > Properties.** The *PoE Properties Page* opens.

STEP 2 Enter the values for the following fields:

- **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.
- **Traps**—Enable or disable traps.

  Traps on the 200 Series switches are syslog related, not SNMP related.
- **Power Trap Threshold**—Enter the usage threshold that is a percentage of the power limit. An alarm is initiated if the power exceeds this value.

The following counters are displayed:

- **Nominal Power**—The total amount of power the switch can supply to all the connected PDs.
- **Consumed Power**—Amount of power currently being consumed by the PoE ports.
- **Available Power**—Nominal power - the amount of consumed power.

Configuring the PoE Power, Priority, and Class

The *PoE Settings Page* displays system PoE information for enabling PoE on the interfaces and monitoring 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 system must be in PoE Port Limit mode. That mode is configured in 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 system must be in PoE Class Limit mode. That mode is configured in the *PoE Properties Page*.

  When the power consumed on the port exceeds the class limit, the port power is turned off.

In some cases, the switch does not have enough power to supply all ports with their allowed power at once. To resolve this problem, assign both limits and priorities to the ports. For example, 15.4W is allowed on all 48 ports, but only 24 ports can be supplied at one time due to power limits. In this case, the priority determines which ports receive power and which ports do not even though no port is above the limit and they all have PDs connected. These priorities are entered in the *PoE Settings Page*.

In the 200 series switches, not all ports are PoE enabled. Use the PoE Settings table to determine which ones support PoE.

To configure PoE port settings:

STEP 1 Click **Port Management > PoE > Settings**. The *PoE Settings Page* opens.

STEP 2 Select a port and click **Edit**. The *Edit PoE Settings Page* opens.

STEP 3 Enter the value for the following field:

- **Port**—Select the port to configure.
- **PoE Administrative Status**—Enable or disable PoE on the port.
- **Max Power Allocation**—Displays the maximum amount of power permitted on this port.

- **Power Priority Level**—Select the port priority: low, high, or critical, for use when the power supply is low. For example, if the power supply is running at 99% usage and port 1 is prioritized as high, but port 3 is prioritized as low, port 1 receives power and port 3 might be denied power.
- **Class**—This field is displayed only if the Power Mode set in the *PoE Properties Page* is Class Limit. The class determines the power level:

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

- **Administrative Power Allocation**—This field is displayed only if the Power Mode set in the *PoE Properties Page* is Port Limit. Enter the power in milliwatts allocated to the port. The range is 0 to 15,400.
- **Power Consumption**—Displays the amount of power in milliwatts assigned to the powered device connected to the selected interface.
- **Overload Counter**—Displays the total number of power overload occurrences.
- Short Counter—Displays the total number of power shortage occurrences.
- **Denied Counter**—Displays number of times the powered device was denied power.
- **Absent Counter**—Displays the number of times that power was stopped to the powered device, because the powered device was no longer detected.
- **Invalid Signature Counter**—Displays the times an invalid signature was received. Signatures are the means by which the powered device identifies itself to the PSE. Signatures are generated during powered device detection, classification, or maintenance.

STEP 4 Click **Apply**. The PoE settings for the port are defined and the switch is updated.

11

VLAN Management

A VLAN is a logical group that enables devices connected to the VLAN 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.

This chapter contains the following topics:

VLANs

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, increasing the maximum frame size from 1518 to 1522. The tag contains a VLAN ID between 1 and 4094, and a VLAN Priority Tag (VPT) between 0 and 7. See *QoS Features and Components* for details about VPT.

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 PVID (Port VLAN Identifier) 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

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

Device VLANs can only be created statically.

Some VLANs can have additional roles, including:

- Voice VLAN: For more information refer to the *Voice VLAN* section.
- Default VLAN: For more information refer to the *Configuring Default VLAN Settings* section.
- Management VLAN: For more information refer to the *IP Addressing* section.

VLAN Configuration Workflow

To configure VLANs:

1. If required, change the default VLAN by using the **Configuring Default VLAN Settings** section.
2. Create the required VLANs by using the **Creating VLANs** section.
3. Set the desired per port VLAN-related configuration using the **Configuring VLAN Interface Settings** section.
4. Assign interfaces to VLANs by using the **Configuring Port to VLAN** section or the **Configuring VLAN to Port** section.
5. You can view the current VLAN port membership for all the interfaces in the **Viewing VLAN Membership** section.

Configuring Default VLAN Settings

At 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:

- It is distinct, non-static/non-dynamic, and all ports are untagged members by default.
- It cannot be deleted.
- It cannot be given a label.
- It cannot be used for any special role, such as unauthenticated VLAN or 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.
- RADIUS servers cannot assign the default VLAN to 802.1x supplicants by using Dynamic VLAN Assignment.

When the VID of the default VLAN is changed, the switch performs the following on all the ports in the VLAN after saving the configuration and rebooting the switch:

- Removes VLAN membership of the ports from the original default VLAN (possible only after reboot).
- Changes the PVID (Port VLAN Identifier) of the ports to the VID of the new default VLAN.
- The original Default VLAN ID is removed from the switch. To be used, it must be recreated.
- 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**. The *Default VLAN Settings Page* opens.

STEP 2 Enter the value for the following field:

- **Current Default VLAN ID**—Displays the current default VLAN ID.
- **Default VLAN ID After Reboot**—Enter a new VLAN ID to replace the default VLAN ID after reboot.

STEP 3 Click **Apply**.

STEP 4 Click **Save** (in the upper-right corner of the window) and save the Running Configuration to the Startup Configuration.

The **Default VLAN ID After Reset** becomes the **Current Default VLAN ID** after you reboot the switch.

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. The Cisco Sx200 Series switch supports 128 VLANs, including the default VLAN.

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 *Create VLAN Page* opens.

The Create VLAN page displays the following fields for all VLANs:

- **VLAN ID**—User-defined VLAN ID.
- **VLAN Name**—User-defined VLAN name.
- **Type**—VLAN type. The possible options are:
  - *Static*—VLAN is user-defined.
  - *Default*—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. The *Add/Edit VLAN Page* opens.

The page enables the creation of either a single VLAN or a range of VLANs.

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

To create a range of VLANs, select the **Range** radio button, and specify the range of VLANs to be created by entering the Starting VID and Ending VID, inclusive.

STEP 4 Click **Apply** to create the VLAN(s).

Configuring VLAN Interface Settings

The *Interface Settings Page* displays and enables configuration of VLAN-related parameters for all interfaces. The Cisco Sx200 Series switch supports 128 VLANs, including the default VLAN.

To configure the VLAN settings:

STEP 1 Click **VLAN Management** > **Interface Settings**. The *Interface Settings Page* opens.

The Interface Settings page lists all ports or LAGs and their VLAN parameters.

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

STEP 3 Select a port or LAG, and click **Edit.** The *Edit Interface Setting Page* opens.

STEP 4 Enter the values for the following fields:

- **Interface**—Select a port/LAG.
- **Interface VLAN Mode**—Select the interface mode for the VLAN. The options are:
  - *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.
- **Administrative PVID**—Enter the Port VLAN ID (PVID) of the VLAN to which incoming untagged and priority tagged frames are classified. The possible values are 1 to 4094.

- **Frame Type**—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 only in General mode) Select to enable ingress filtering. When an interface is ingress filtering enabled, the interface discards all incoming frames that are classified as VLANs of which the interface is not a member. Ingress filtering can be disabled or enabled on general ports. It is always enabled on access ports and trunk ports.
- **Auto Membership in Voice VLAN**—Select to enable Auto Voice VLAN Membership. When this option is enabled on an interface, the switch automatically configures the interface as a member of the Voice VLAN, if the switch detects incoming voice packets based on configured telephony Organizationally Unique Identifiers (OUIs). LLDP-MED network policy does not activate Voice VLAN.
- **Voice VLAN QoS Mode**—Select one of the following values:
  - *All*—Quality of Service (QoS) values configured to the Voice VLAN are applied to all the incoming frames that are received on the interface and are classified to the Voice VLAN.
  - *Telephony Source MAC* Address—The QoS values configured for the Voice VLAN are applied to any incoming frame that is received on the interface, is classified to the Voice VLAN, and has a source MAC address that is configured with telephony OUI. (Telephony OUIs are configured by using the procedure in the **Configuring Telephony OUI** section.)

STEP 5 Click **Apply**. The parameters are set, and the switch is updated.

Defining VLAN Membership

The **Port to VLAN Page**, *VLAN To Port Page,* and *Port VLAN Membership Page* display the VLAN memberships of the ports in various presentations. You can use the **Port to VLAN Page** and the *VLAN To Port Page* to add or remove memberships to or from the VLANs.

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 packets properly, intermediate VLAN-aware devices that carry VLAN traffic along the path between end nodes must be manually configured.

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.

VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices. 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. That is, the egress port that reaches the end node must be an untagged member of the VLAN.

Configuring Port to VLAN

Use the **Port to VLAN Page** to display and configure a VLAN and all its port members on a single page.

To map ports or LAGs to a VLAN:

STEP 1 Click **VLAN Management** > **Port to VLAN**. The **Port to VLAN Page** opens.

STEP 2 Select a VLAN and the interface type (Port or LAG), and click **Go** to display or to change the port characteristic with respect to the VLAN.

The port mode for each port or LAG is displayed with its current port mode (Access, Trunk or General) configured from the *Interface Settings Page*.

Each port or LAG is displayed with its current registration to the VLAN.

STEP 3 Change the registration of an interface to the VLAN by selecting the desired option from the following list:

- **Forbidden**—The interface is not allowed to join the VLAN. 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 when the VLAN is newly created.
- **Tagged**—The interface is a tagged member of the VLAN. Frames of the VLAN are sent tagged to the interface VLAN.
- **Untagged**—The interface is an untagged member of the VLAN. Frames of the VLAN are sent untagged to the interface VLAN.
- **PVID**—Select 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 switch is updated.

You can continue to display and/or configure port membership of another VLAN by selecting another VLAN ID.

Configuring VLAN to Port

Use the *VLAN To Port Page* to map ports to multiple dynamic VLANs.

To assign a port to multiple VLANs:

STEP 1 Click **VLAN Management** > **VLAN to Port**. The *VLAN To Port Page* opens.

STEP 2 Select interface type (Port or LAG), and click **Go**. The following fields are displayed for all interfaces of the selected type:

- **Interface**—Port/LAG ID.
- **Mode**—Interface VLAN mode that was selected in the *Interface Settings Page.*

- **VLANs**—Drop-down list that displays all VLANs of which the interface is a member.
- **LAG**—If interface selected is Port, displays the LAG in which it is a member.

STEP 3 Select a port, and click the **Join VLAN** button. The *Join VLAN To Port Page* opens.

STEP 4 Enter the values for the following fields:

- **Interface**—Select a Port or LAG.
- **Mode**—Displays the port VLAN mode that was selected in the *Interface Settings Page*.
- **Select VLAN**—To associate a port with a VLAN(s), move the VLAN ID(s) 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/PVID options:
  - *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 switch is updated.

Viewing VLAN Membership

The *Port VLAN Membership Page* displays a list of VLANs to which each port belongs. If the port-based authentication method for an interface is 802.1x and the Administrative Port Control is Auto, then:

- Until the port is authenticated, it is excluded from all VLANs, except guest and unauthenticated ones. In the VLAN to Port page, the port will be marked with “P”.
- When the port is authenticated, it receives membership in the VLAN in which it was configured.

To view VLAN membership:

STEP 1 Click **VLAN Management** > **Port VLAN Membership**. The *Port VLAN Membership Page* opens.

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

The Port VLAN Membership page displays the operational membership of the ports or LAGs:

- **Port** number.
- **Mode**—Port mode defined in the *Interface Settings Page*.
- **PVID**—Port VLAN Identifier of the VLAN to which incoming untagged frames are assigned at ingress. This assumes that no other VLAN assignment mechanism is used, such as MAC-based-VLAN.
- **VLANs**—VLAN to which the port belongs.

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 QoS (Quality of Service) to packets from the Voice VLAN.

QoS attributes can be assigned to VoIP packets (both voice and signaling), to prioritize the traffic through the switch. The QoS attributes can be assigned per port to the voice packets in two modes:

- **All**—Quality of Service (QoS) values configured to the Voice VLAN are applied to all of the incoming frames that are received on the interface and are classified to the Voice VLAN.
- **SRC**—The QoS values configured for the Voice VLAN are applied to any incoming frame that is received on the interface, is classified to the Voice VLAN, and has a source MAC address that is configured with telephony OUI. (Telephony OUIs are configured by using the procedure in the **Configuring Telephony OUI** section.)

In MAC addresses, the first three bytes contain a manufacturer ID, known as an Organizationally Unique Identifier (OUI), and the last three bytes contain a unique station ID. The classification of a packet from VoIP equipment or phones is based on the OUI of the packet source MAC address.

Ports can be assigned to Voice VLAN as follows:

- **Static**—Assigned manually to the Voice VLAN (described in the **Configuring VLAN Interface Settings** section).
- **Dynamic**—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. (This is configured by using the process described in the **Configuring VLAN Interface Settings** section.) 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. The aging time can be changed by using the procedure described in the **Configuring Voice VLAN Properties** section.

The following network scenarios are supported for dynamic assignment:

- A phone is configured with the Voice VLAN ID, and always sends tagged packets.
- A phone sends untagged packets to acquire its initial IP address. A response from the local DHCP server directs the phone to use the Voice VLAN ID. The phone then restarts a DHCP session on the Voice VLAN (tagged).
- If the voice equipment supports the LLDP-MED protocol, the switch sends a LLDP-MED network policy that tells the phone to how to send frames to the switch (for example: tagged, and tagged with what VLAN).

Voice VLAN Options

You can perform the following operations with this feature:

- Enable or disable Voice VLAN as described in the **Configuring Voice VLAN Properties** section.
- Create a new VLAN to serve as the Voice VLAN by using the *Create VLAN Page*, or configure an existing VLAN as described in the **Configuring Voice VLAN Properties** section.

- Assign ports as candidates to the Voice VLAN. (This is configured by using the process described in the **Configuring VLAN Interface Settings** section.)
- Assign the QoS mode per port to one of the following:
  - For a port that has already joined the Voice VLAN, all packets are assigned to the Voice VLAN as described in the **Configuring VLAN Interface Settings** section.
  - Only packets that come from IP phones (based on the source OUI MAC address prefix) by using the procedure described in the **Configuring VLAN Interface Settings** section.
- Enter Voice VLAN Class of Service (with or without remarking the packet VPT) by using the *Voice VLAN Properties Page*. When remark is selected, the switch changes the 802.1p priority of the packet at egress. Set the remarking option as described in the **Configuring Voice VLAN Properties** section.
- Configure and update the Telephony OUI table with up to 128 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.
- Enter the Voice VLAN aging time as described in the **Configuring Voice VLAN Properties** section.

Voice VLAN Constraints

The following constraints exist:

- Only one Voice VLAN is supported.
- The Voice VLAN is not supported by DVA (Dynamic VLAN assignment).
- The Voice VLAN must be a static VLAN created manually.
- A VLAN that is defined as a Voice VLAN cannot be removed.
- A new VLAN ID can be configured for the Voice VLAN only if the current Voice VLAN does not have candidate ports.
- 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 decision.

- The Voice VLAN QoS is applied to candidate ports that have joined the Voice VLAN, and to static ports.
- The voice flow is accepted if the MAC address can be learned by the FDB. (If there is no free space in FDB, no action occurs).

Configuring Voice VLAN Properties

Use the *Voice VLAN Properties Page* to globally configure the Voice VLAN feature by configuring the following:

- VLAN ID of the Voice VLAN
- Traffic-class received by the traffic
- Time interval that the port remains in the Voice VLAN after the last VoIP frame is identified as having an OUI in the table

To enable the feature on a port, it must be globally enabled in the *Interface Settings Page*.

To configure Voice VLAN properties:

STEP 1 Click **VLAN Management** > **Voice VLAN** > **Properties**. The *Voice VLAN Properties Page* opens.

STEP 2 Enter the values for the following fields:

- **Voice VLAN Status**—Select this field to enable the Voice VLAN feature.
- **Voice VLAN ID**—Select the VLAN that is to be the Voice VLAN.
- **Class of Service**—Select to add a CoS level to untagged packets received on the Voice VLAN. 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).
- **Remark CoS**—Select to reassign the CoS level to packets received on the Voice VLAN. If this option is selected, the outer user priority will be the new CoS. Otherwise, the outer user priority will be the original CoS, since Trust mode is used.
- **Auto Membership Aging Time**—Enter the interval of time after which the port exits the voice VLAN, if no voice packets are received. The range is from 1 minute to 30 days.

STEP 3 Click **Apply**. The VLAN properties are saved, and the switch 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 causes 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 128 OUIs.

Use the *Telephony OUI Page* to view existing OUIs, and add new OUIs.

To add a new Voice VLAN OUI:

STEP 1 Click **VLAN Management** > **Voice VLAN** > **Telephony OUI**. The *Telephony OUI Page* opens.

The Telephone OUI page displays the following fields:

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

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

To delete all the OUIs, select the top checkbox. All the OUIs are selected and can be deleted by clicking **Delete**. If you then click **Restore**, the system recovers the known OUIs.

STEP 2 Click **Add.** The *Add Telephony OUI Page* opens.

STEP 3 Enter the values for the following fields:

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

STEP 4 Click **Apply**. The OUI is added.

12

Configuring the Spanning Tree Protocol

The Spanning Tree Protocol (STP) (IEEE802.1D and IEEE802.1Q) is enabled by default, set to RSTP (Rapid Spanning Tree Protocol) mode, and 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 do not transfer user data. They are automatically re-activated when the topology changes to make it desirable to transfer user data.

This chapter contains the following topics:

STP Flavors

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause Layer 2 switches to forward traffic indefinitely, resulting in increased traffic and reduced network efficiency.

STP provides a tree topology for any arrangement of Layer 2 switches and interconnecting links, creating a unique path between end stations on a network, eliminating loops.

The switch supports the following Spanning Tree Protocol versions:

- Classic STP provides a single path between any two end stations, avoiding and eliminating loops.
- Rapid STP (RSTP) detects network topologies to provide faster convergence of the spanning tree. This is most effective when the network topology is naturally tree-structured, and therefore faster convergence might be possible. RSTP is enabled by default.

  Although Classic STP is guaranteed to prevent Layer 2 forwarding loops in a general network topology, there might be an unacceptable delay before convergence. This means that each bridge or switch in the network needs to decide, if it should actively forward traffic or not on each of its ports.

  NOTE The 200 Series switches do not support MSTP.

Configuring STP Status and Global Settings

The STP Status and Global Settings Page contains parameters for enabling STP or RSTP.

Use the STP Interface Settings Page and RSTP Interface Settings Page to configure each mode, respectively.

To set STP status and global settings:

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

STEP 2 Enter the parameters:

Global Settings:

- **Spanning Tree State**—Enable or disable STP on the switch.
- **STP Operation Mode**—Select an STP mode.
- B**ridge Protocol Data Unit (BPDU) Handling**—Select how BPDU packets are managed when STP is disabled on the port or the switch. BPDUs are used to transmit spanning tree information.
  - Filtering—Filters BPDU packets when Spanning Tree is disabled on an interface.

  - Flooding—Floods BPDU packets when Spanning Tree is disabled on an interface.

- **Path Cost Default Values**—Selects the method used to assign default path costs to the STP ports. The default path cost assigned to an interface varies according to the selected method.
  - Short—Specifies that the default port path costs are within the range: 1—65,535.
  - Long—Specifies that the default port path costs are within the range: 1—200,000,000.

Bridge Settings:

- **Priority**—Sets the bridge priority value. After exchanging BPDUs, the device with the lowest priority becomes the Root Bridge. In the case that all bridges use the same priority, then their MAC addresses are used to determine 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**—Set the interval in seconds that a Root Bridge waits between configuration messages. The range is 1 to 10 seconds.
- **Max Age**—Set the interval in seconds that the switch can wait without receiving a configuration message, before attempting to redefine its own configuration.
- **Forward Delay**—Set the interval in seconds that a bridge remains in a learning state before forwarding packets. For more information, refer to *Defining Spanning Tree Interface Settings*.

Designated Root:

- **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 3 Click **Apply**. The switch is updated with the STP Global settings.

Defining Spanning Tree Interface Settings

The STP Interface Settings Page enables you to configure STP on a per-port basis, and to view the information learned by the protocol, such as the designated bridge.

The configuration entered on this page is active for all flavors of the STP protocol.

To configure STP on an interface:

STEP 1 Click **Spanning Tree** > **STP Interface Settings**. The *STP Interface Settings Page* displays.

STEP 2 Select an interface and click **Edit**. The Edit Interface Settings Page displays.

STEP 3 Enter the parameters

- **Interface**—Select the port number or LAG on which Spanning Tree is configured.
- **STP**—Enables or disables STP on the port.
- **Edge Port**—Enables or disables Fast Link on the port. If Fast Link mode is enabled for a port, the port state is automatically placed in the Forwarding state when the port link is up. Fast Link optimizes the STP protocol convergence. The options are:
  - Enable—Enables Fast Link immediately.
  - Auto—Enables Fast Link a few seconds after the interface becomes active. This allows STP to resolve loops before enabling Fast Link.
  - Disable—Disables Fast Link.
- **BPDU Handling**—Select how BPDU packets are managed when STP is disabled on the port or the switch. BPDUs are used to transmit spanning tree information.

  - Use Global Settings—Select to use the settings defined in the **STP Status and Global Settings Page**.
  - Filtering—Filters BPDU packets when Spanning Tree is disabled on an interface.
  - Flooding—Floods BPDU packets when Spanning Tree is disabled on an interface.
- **Path Cost**—Set the port contribution to the root path cost or use the default cost generated by the system.
- **Priority**—Set the priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority is a value from 0 to 240, set in increments of 16.
- **Port State**—Displays the current STP state of a port.
  - Disabled—STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
  - Blocking—The port is currently blocked, and cannot forward traffic (with the exception of BPDU data) or learn MAC addresses.
  - Listening—The port is in Listening mode. The port cannot forward traffic, and cannot learn MAC addresses.
  - Learning—The port is in Learning mode. The port cannot forward traffic, but it can learn new MAC addresses.
  - Forwarding—The port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Port Role**—Displays the behavior of the port.
- **Designated Bridge ID**—Displays the bridge priority and the MAC address of the designated bridge.
- **Designated Port ID**—Displays the priority and interface of the selected port.
- **Designated Cost**—Displays the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- **Forward Transitions**—Displays the number of times the port has changed from the **Blocking** state to **Forwarding** state.
- **Speed**—Displays the speed of the port.

- **LAG**—Displays the LAG to which the port belongs. If a port is a member of a LAG, the LAG settings override the port settings.

STEP 4 Click **Apply**. The interface settings are modified, and the switch is updated.

Configuring Rapid Spanning Tree Settings

Rapid Spanning Tree Protocol (RSTP) detects and uses network topologies that enable a faster STP convergence without creating forwarding loops.

The RSTP Interface Settings Page enables you to configure RSTP per port. Any configuration that is done on this page is active when the global STP mode is set to RSTP.

To enter RSTP settings:

STEP 1 Click **Spanning Tree** > **STP Status and Global Settings**. The *STP Status and Global Settings Page* displays. Enable **RSTP**.

STEP 2 Click **Spanning Tree** > **RSTP Interface Settings**. The RSTP Interface Settings Page opens:

STEP 3 Select a port. (Activate Protocol Migration is only available after selecting the port connected to the bridge partner being tested.)

STEP 4 If a link partner is discovered by using STP, click **Activate Protocol Migration** to run a Protocol Migration test. This discovers whether the link partner using STP still exists, and if so whether it has migrated to RSTP . If it still exists as an STP link, the device continues to communicate with it by using STP.

STEP 5 Select an interface, and click **Edit**. The *Edit Rapid Spanning Tree Page* displays.

STEP 6 Enter the parameters

- **Interface**—Set the interface, and specify the port or LAG where RSTP is to be configured.
- **Point-to-Point Administrative Status**—Define the point-to-point link status. Ports defined as Full Duplex are considered Point-to-Point port links.
  - Enable—This port is a RSTP edge port when this feature is enabled, and brings it to Forwarding mode quickly (usually within 2 seconds).

  - Disable—The port is not considered point-to-point for RSTP purposes, which means that STP works on it at regular speed, as opposed to rapid speed.
  - Auto—Automatically determines switch status by using RSTP BPDUs.
- **Point-to-Point Operational Status**—Displays the Point-to-Point operating status if the **Point-to-Point Administrative Status** is set to Auto.
- **Role**—Displays the role of the port 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 interface 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.
- **Mode**—Displays the current Spanning Tree mode: Classic STP or RSTP.
- **Fast Link Operational Status**—Displays whether the Fast Link (Edge Port) is enabled, disabled, or automatic for the interface. The values are:
  - Enabled—Fast Link is enabled.
  - Disabled—Fast Link is disabled.
  - Auto—Fast Link mode is enabled a few seconds after the interface becomes active.
- **Port Status**—Displays the RSTP status on the specific port.
  - Disabled—STP is currently disabled on the port.
  - Blocking—The port is currently blocked, and it cannot forward traffic or learn MAC addresses.
  - Listening—The port is in Listening mode. The port cannot forward traffic, and cannot learn MAC addresses.

- Learning—The port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
- Forwarding—The port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.

STEP 7 Click **Apply**. The switch is updated.

13

Managing MAC Address Tables

MAC addresses are stored in the *Static Address* table or the *Dynamic Address* table, along with VLAN and port information. Static addresses are configured by the user in the Static Address table and do not age out. MAC addresses seen in packets arriving at the switch are listed in the Dynamic Address table for a period of time. If another frame with the same source MAC address does not appear on the switch before that time expires, the entry is deleted from the table.

When a frame arrives on the switch, the switch searches for a MAC address that matches a static or dynamic table entry. If a match is found, the frame is marked for egress on a specific port based on the search of the tables. Frames addressed to a destination MAC address that is not found in the tables are flooded to all the ports on the relevant VLAN. These frames are called Unknown Unicast Frames.

The switch supports a maximum of 8,000 of static and dynamic MAC addresses.

This section contains information for defining both static and dynamic MAC address tables and includes the following topics:

- **Configuring Static MAC Addresses**
- **Dynamic MAC Addresses**

Configuring Static MAC Addresses

Static addresses can be assigned to a specific interface and VLAN on the switch. The addresses are bound to the assigned interface. If a static address is seen on another interface, the address is ignored and it is not written to the address table.

The *Static Addresses Page* enables viewing statically-configured MAC addresses and creating new static MAC addresses.

To define a static address:

STEP 1 Click **MAC Address Tables > Static Addresses**. The *Static Addresses Page* opens.

The *Static Addresses Page* displays the defined static addresses.

STEP 2 Click **Add**. The *Add Static Address Page* opens.

STEP 3 Enter the parameters.

- **VLAN ID**—Select the VLAN ID for the port.
- **MAC Address**—Enter the interface MAC address.
- **Interface**—Select an interface (port or LAG) for the entry.
- **Status**—Select how the entry is treated. The options are:
  - *Permanent*—The static MAC address is never aged out of the table and if it is saved to the Startup Configuration, it is retained after rebooting.
  - *Delete on reset*—The static MAC address is never aged out of the table
  - *Delete on timeout*—The MAC address is deleted when aging occurs.
  - *Secure*—The MAC address is secure when the interface is in classic locked mode.

STEP 4 Click **Apply**. A new entry is made in the table.

Dynamic MAC Addresses

The Dynamic Address Table contains the MAC addresses acquired by monitoring the source addresses of traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports in the VLAN of the frame.

To prevent the bridging table from overflowing and to make room for new addresses, an address is deleted from the bridging table if no traffic is received from a dynamic MAC address for a certain period. This period of time is the aging interval.

Configuring Dynamic MAC Address Parameters

The *Dynamic Addresses Setting Page* enables entering the aging interval for the MAC address table.

To enter the aging interval for dynamic addresses:

STEP 1 Click **MAC Address Tables > Dynamic Address Settings**. The *Dynamic Addresses Setting Page* opens.

STEP 2 Enter **Aging Time**. The aging time is a value between the user-configured value and twice that value minus 1. For example, if you entered 300 seconds, the aging time is between 300 and 599 seconds.

STEP 3 Click **Apply**. The Dynamic MAC Address Table is updated.

Querying Dynamic Addresses

The *Dynamic Addresses Page* enables querying the Dynamic MAC Address table according to the following criteria:

- Interface type
- MAC addresses
- VLAN

This page displays the dynamically-learned MAC addresses. You can clear the dynamic addresses from the MAC address table and specify the 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 are entered, the entire table is displayed.

To perform query dynamic addresses:

STEP 1 Click **MAC Address Tables > Dynamic Addresses**. The *Dynamic Addresses Page* opens.

STEP 2 In the *Filter* block, enter the following query criteria:

- **VLAN ID**—Enter the VLAN ID for which the table is queried.
- **MAC Address**—Enter the MAC address for which the table is queried.

- **Interface**—Select the interface for which the table is queried. The query can search for specific ports or LAGs.
- **Dynamic Address Table Sort Key**—Enter the field by which the table is sorted. The address table can be sorted by VLAN ID, MAC address, or interface.

STEP 3 Select the preferred option for sorting the addresses table in the Dynamic Address Sort Key.

STEP 4 Click **Go**. The Dynamic MAC Address Table is queried and the results are displayed.

Click **Clear Table** to delete all of the dynamic MAC addresses.

14

Configuring Multicast Forwarding

This chapter describes the Multicast Forwarding feature, and contains 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 switch 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 that 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 where it receives the Join messages wants to receive a specific Multicast stream. The Mrouter forwards the requested Multicast stream to the interface.

Multicast Operation

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 based on one of the following options:

- Multicast MAC Group Address
- IP Multicast Group Address (G)
- A combination of the source IP address (S) and the destination IP Multicast Group Address (G) of the Multicast packet.

One of these options can be configured per VLAN.

The system 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

Multicast registration is the process of listening and responding to Multicast registration protocols. The available protocols are the IGMP for IPv4 and the MLD protocol for IPv6.

When IGMP/MLD snooping is enabled in a switch on a VLAN, it analyzes all of the IGMP/MLD packets it receives from the VLAN connected to the switch and Multicast routers in the network.

When a switch learns that a host is using IGMP/MLD messages to register to receive a Multicast stream, optionally from a specific source, the switch adds the registration in its Multicast forwarding data base.

IGMP/MLD snooping can effectively reduce Multicast traffic from streaming bandwidth-intensive IP applications. A switch 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 switch, and also reduces the workload at 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

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 which 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 them with 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.

Defining Multicast Properties

The *Properties Page* enables you to configure the Bridge Multicast filtering status.

By default, all Multicast frames are flooded to all port of the VLAN. To selectively forward only to relevant ports and filter (drop) the Multicast on the rest of the ports, enable Bridge Multicast filtering status in the *Properties Page.*

If filtering is enabled, Multicast frames are forwarded to a subset of the ports in the relevant VLAN as defined in the Multicast Forwarding Data Base (MFDB). Multicast filtering is enforced on all traffic. By default, such traffic is flooded to all relevant ports, but you can limit forwarding to a smaller subset.

A common way of representing Multicast membership is the (S,G) notation where "S" is the (single) source sending a Multicast stream of data, and "G" is the IPv4 or IPv6 group address. If a Multicast client can receive Multicast traffic from any source of a specific Multicast group, this is written as (*,G).

The following are ways of forwarding Multicast frames:

- **MAC Group Address**—Based on the destination MAC in the Ethernet frame.

  NOTE As mentioned in the Multicast Address Properties section, one or more IP Multicast group addresses can be mapped into a MAC group address. Forwarding based on MAC group address can result in an IP Multicast stream being forwarded out to ports that have no receiver for the stream.

- **IP Group Address**—Based on the destination IP address of the IP packet (*,G).
- **Source Specific IP Group Address**—Based on both the destination IP address and the source IP address of the IP packet (S,G).

By selecting the forwarding mode, you can define the method used by hardware to identify Multicast flow by one of the following options: MAC Group Address, IP Group Address, or Source Specific IP Group Address.

(S,G) is supported by IGMPv3 and MLDv2, while IGMPv1/2 and MLDv1 support only (*.G) which is just the group ID.

The switch supports a maximum of 256 static and dynamic Multicast group addresses.

To enable Multicast filtering, and select the forwarding method:

STEP 1 Click **Multicast> Properties**. The *Properties Page* opens.

STEP 2 Enter the parameters.

- **Bridge Multicast Filtering Status**—Enable or disable filtering.
- **VLAN ID**—Select the VLAN ID to set its forwarding method.
- **Forwarding Method for IPv6**—Set the forwarding method for IPv6 addresses. These are used by hardware to identify Multicast flow by one of the following options: MAC Group Address, IP Group Address, or Source Specific IP Group Address.

- **Forwarding Method for IPv4**—Set the forwarding method for IPv4 addresses. These are used by hardware to identify Multicast flow by one of the following options: MAC Group Address, IP Group Address, or Source Specific IP Group Address.

STEP 3 Click **Apply**. The switch is updated.

Adding MAC Group Address

The switch supports forwarding incoming Multicast traffic based on the Multicast group information. This information is derived from the IGMP/MLD packets received or as the result of manual configuration, and stored in the Multicast Forwarding Database (MFDB).

When a frame is received from a VLAN that is configured to forward Multicast streams based on MAC group addresses, and its destination address is a Layer 2 Multicast address, the frame is forwarded to all ports that are members of the MAC group address.

The *MAC Group Address Page* has the following functions:

- Query and view information from the Multicast Filtering Database relating to a specific VLAN ID or a specific MAC address group. This data is acquired either dynamically through IGMP/MLD snooping or statically by manual entry.
- Add or delete static entries to this database which provides static forwarding information based on MAC destination addresses.
- Display a list of all ports/LAGs that are a member for each VLAN ID and MAC address group, and enter whether traffic is forwarded to it or not.

For viewing the forwarding information when the mode is *IP Address Group* or *IP and Source Group*, use the *IP Multicast Group Address Page*.

To define and view MAC Multicast groups:

STEP 1 Click **Multicast> MAC Group Address**. The *MAC Group Address Page* opens.

STEP 2 Enter the parameters.

- **VLAN ID Equals To**—Set the VLAN ID of the group to be displayed.

- **MAC Group Address Equals To**—Set the MAC address of the Multicast group to be displayed. If no MAC Group Address is specified, the page displays all the MAC Group Addresses from the selected VLAN.

STEP 3 Click **Go,** and the MAC Multicast group addresses are displayed in the lower block.

STEP 4 Click **Add** to add a static MAC Group Address. The *Add MAC Group Address Page* opens.

STEP 5 Enter the parameters.

- **VLAN ID**—Defines the VLAN ID of the new Multicast group.
- **MAC Group Address**—Defines the MAC address of the new Multicast group.

STEP 6 Click **Apply**, the MAC Multicast group is added, and the switch is updated.

To configure and display the registration for the interfaces within the group, select an address, and click **Details.** The *MAC Group Address Settings Page* opens.

The page displays:

- **VLAN ID**—The VLAN ID of the Multicast group.
- **MAC Group Address**—The MAC address of the group.

STEP 7 Select the port or LAG to be displayed from the **Filter: Interface Type** menu.

STEP 8 Click **Go** to display the port or LAG membership.

STEP 9 Select the way that each interface is associated with the Multicast group:

- **Static**—Attaches the interface to the Multicast group as a static member.
- **Forbidden**—Specifies that this port is forbidden from joining this group on this VLAN.
- **None**—Specifies that the port is not currently a member of this Multicast group on this VLAN.

STEP 10 Click **Apply**, and the switch is updated.

Adding IP Multicast Group Addresses

The *IP Multicast Group Address Page* is similar to the *MAC Group Address Page* except that Multicast groups are identified by IP addresses.

The *IP Multicast Group Address Page* enables querying and adding IP Multicast groups.

To define and view IP Multicast groups:

STEP 1 Click **Multicast> IP Multicast Group Address**. The *IP Multicast Group Address Page* opens.

The page displays all of the IP Multicast group addresses learned by snooping.

STEP 2 Enter the parameters required for filtering.

- **VLAN ID equals to**—Define the VLAN ID of the group to be displayed.
- **IP Version equals to**—Select IPv6 or IPv4.
- **IP Multicast Group Address equals to**—Define the IP address of the Multicast group to be displayed. This is only relevant when Forwarding mode is (S,G).
- **Source IP Address equals to**—Define the source IP address of the sending device. If mode is (S,G), enter the sender S. This together with the IP Group Address is the Multicast group ID (S,G) to be displayed. If mode is (*.G), enter an * to indicate that the Multicast group is only defined by destination.

STEP 3 Click **Go**. The results are displayed in the lower block. When Bonjour and IGMP are enabled, the IP Multicast address of Bonjour is displayed.

STEP 4 Click **Add** to add a static IP Multicast Group Address. The IP Multicast Interface Settings Page opens.

STEP 5 Enter the parameters.

- **VLAN ID**—Defines the VLAN ID of the group to be added.
- **IP Version**—Select the IP address type.
- **IP Multicast Group Address**—Define the IP address of the new Multicast group.
- **Source Specific**—Indicates that the entry contains a specific source, and adds the address in the IP Source Address field. If not, the entry is added as a (*,G) entry, an IP group address from any IP source.

- **IP Source Address**—Defines the source address to be included.

STEP 6 Click **Apply**. The IP Multicast group is added, and the device is updated.

STEP 7 To configure and display the registration of an IP group address, select an address and click **Details**. The IP Multicast Interface Settings Page opens.

STEP 8 Use the filter "Interface Type equals" to view the group membership on port or LAG and click **Go**.

STEP 9 For each interface, select its association type. The options are as follows:

- *Static*—Attaches the interface to the Multicast group as a static member.
- *Dynamic*—Indicates that the interface was added to the Multicast group as a result of IGMP/MLD snooping.
- *Forbidden*—Specifies that this port is forbidden from joining this group on this VLAN.
- *None*—Indicates that the port is not currently a member of this Multicast group on this VLAN.

STEP 10 Click **Apply**. The switch is updated.

Configuring IGMP Snooping

To support selective Multicast forwarding (IPv4), Bridge Multicast filtering must be enabled, and IGMP Snooping must be enabled globally and for each relevant VLAN.

By default, a Layer 2 switch forwards Multicast frames to all ports of the relevant VLAN, essentially treating the frame as if it were a Broadcast. With IGMP Snooping the switch forwards Multicast frames to ports that have registered Multicast clients.

NOTE The switch supports IGMP Snooping only on static VLANs. It does not support IGMP Snooping on 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, DVMRP, or IGMP query protocols.

These are displayed on the *IGMP Snooping Page*.

Ports asking to join a specific Multicast group issue an IGMP report that specifies which group(s) the host wants to join. This results in the creation of a forwarding entry in the Multicast forwarding database.

To enable IGMP Snooping on a VLAN:

STEP 1 Click **Multicast** > **IGMP Snooping**. The *IGMP Snooping Page* opens.

The IGMP Snooping Table displays the IGMP snooping information for the VLANs on the switch. The columns are described in **STEP 4**.

STEP 2 Check Enable for IGMP Snooping status.

IGMP Snooping Status globally enables the device monitoring network traffic to determine which hosts have requested to receive Multicast traffic. The switch performs IGMP Snooping if IGMP snooping and Bridge Multicast filtering are both enabled.

STEP 3 Select a VLAN, and click **Edit**. The *Edit IGMP Snooping Page* opens.

There should be only one IGMP Querier in a network. The switch supports standards-based IGMP Querier election. The following values are used when the querier message does not supply them (for IGMPv1/v2).

STEP 4 Enter the parameters.

- **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. The switch performs IGMP snooping only if IGMP snooping and Bridge Multicast filtering are both enabled.

- **Operational IGMP Snooping Status**—Displays the current status of the IGMP Snooping for the selected VLAN.
- **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.
- **Operational Query Robustness**—Displays the robustness variable sent by the elected querier.
- **Query Interval**—Enter the interval between the General Queries to be used.
- **Operational Query Interval**—The time interval in seconds between General Queries sent by the elected querier.
- **Query Max Response Interval**—Enter the delay used to calculate the Maximum Response Code inserted into the periodic General Queries.
- **Operational Query Max Response Interval**—Displays the Query Max Response Interval included in the General Queries sent by the elected querier.
- **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.
- **Operational Last Member Query Counter**—Displays the operational value of the Last Member Query Counter.
- **Last Member Query Interval**—Enter the Maximum Response Delay to be used if the switch cannot read Max Response Time value from Group-Specific queries sent by the elected querier.
- **Operational Last Member Query Interval**—Displays the Last Member Query Interval sent by the elected querier.
- **Immediate Leave**—Enable 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.

STEP 5 Click **Apply**. The switch is updated.

MLD Snooping

When IGMP/MLD snooping is enabled in a switch on a VLAN, it analyzes all of the IGMP/MLD packets it receives from the VLAN connected to the switch and Multicast routers in the network.

When a switch learns that a host is using IGMP/MLD messages to register to receive a Multicast stream, optionally from a specific source, the switch adds the registration in its Multicast forwarding data base.

IGMP/MLD snooping can effectively reduce Multicast traffic from streaming bandwidth-intensive IP applications. A switch 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 switch, and also reduces the workload at 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

To support selective Multicast forwarding (IPv6), Bridge Multicast filtering must be enabled, and MLD Snooping must be enabled globally and for each relevant VLAN.

NOTE The switch supports MLD Snooping only on static VLANs. It does not support MLD Snooping on dynamic VLANs

The switch uses this feature to build Multicast membership lists. It uses the 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.

Hosts use the MLD protocol to report their participation in Multicast sessions.

The switch supports two versions of MLD snooping:

- 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 source IPv6 address, and the destination IPv6 Multicast address.

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 system is rebooted.

To enable MLD Snooping:

STEP 1 Click **Multicast** > **MLD Snooping**. The *MLD Snooping Page* opens.

STEP 2 Enable or disable **MLD Snooping Status.** MLD Snooping Status globally enables the device monitoring network traffic to determine which hosts have requested to receive Multicast traffic. The switch performs MLD Snooping if MLD snooping and Bridge Multicast filtering are both enabled.

The MLD Snooping Table block lists the operational MLD snooping information for the VLANs on the switch. For a description of the table columns, see **STEP 3**.

STEP 3 Select a VLAN, and click **Edit**. The *Edit MLD Snooping Page* opens.

STEP 4 Enter the parameters.

- **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 and Bridge Multicast filtering are both enabled.
- **Operational MLD Snooping Status**—Displays the current status of MLD Snooping for the selected VLAN.
- **MRouter Ports Auto-Learn**—Enable or disable Auto Learn for 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.
- **Operational Query Robustness**—Displays the robustness variable 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.
- **Operational Query Interval**—The time interval in seconds between General Queries received from the elected querier.
- **Query Max Response Interval**—Enter Query Max Response delay to be used if the switch cannot read the Max Response Time value from General Queries sent by the elected querier.
- **Operational Query Max Response Interval**—Displays the delay used to calculate the Maximum Response Code inserted into the General Queries.
- **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.
- **Operational Last Member Query Counter**—Displays the operational value of the Last Member Query Counter.
- **Last Member Query Interval**—Enter the Maximum Response Delay to be used if the switch cannot read Max Response Time value from Group-Specific queries sent by the elected querier.
- **Operational Last Member Query Interval**—The Last Member Query Interval sent by the elected querier.
- **Immediate Leave**—When enabled, reduces the time it takes to block unnecessary MLD traffic sent to a switch port.

STEP 5 Click **Apply**. The switch is updated.

Viewing IGMP/MLD IP Multicast Groups

The IGMP/MLD IP Multicast Group Page displays the IPv4 and IPv6 group address the switch learned from the IGMP/MLD messages it snoops.

There might be a difference between information on this page and, for example, information displayed in the *MAC Group Address Page.* Assuming that the system is in MAC-based groups and a port that requested to join the following Multicast groups 224.1.1.1 and 225.1.1.1, both are mapped to the same MAC Multicast address 01:00:5e:01:01:01. In this case, there is a single entry in the MAC Multicast page, but two entries on this page.

To query for a IP Multicast group:

STEP 1 Click **Multicast** > **IGMP/MLD IP Multicast Group**. The *IGMP/MLD IP Multicast Group Page* opens.

STEP 2 Set the type of snooping group for which to search: IGMP or MLD.

STEP 3 Enter some or all of following query filter criteria:

- **Group Address equals to**—Defines the Multicast group MAC address or IP address to query.
- **Source Address equals to**—Defines the sender address to query.
- **VLAN ID equals to**—Defines the VLAN ID to query.

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

- **VLAN**—The VLAN ID.
- **Group Address**—The Multicast group MAC address or IP address.
- **Source Address**—The sender address for all of the specified group ports.
- **Included Ports**—The list of ports to where the corresponding Multicast stream is forwarded.
- **Excluded Ports**—The list of ports not included in the group.
- **Compatibility Mode**—The oldest IGMP/MLD version of registration from the hosts the switch receives on the IP group address.

Defining Multicast Router Ports

A Multicast router (Mrouter) port is a port that connects to a Multicast router. The switch includes the Multicast router port(s) when it forwards the Multicast streams and IGMP/MLD registration messages. This is required in order for all the Multicast routers can in turn forward the Multicast streams and propagate the registration messages to other subnets.

On this page, it is possible to statically configure or dynamically detect which ports are connected to Mrouters.

To define Multicast router ports:

STEP 1 Click **Multicast** > **Multicast Router Port**. The *Multicast Router Port Page* opens.

STEP 2 Enter some or all of following query filter criteria:

- **VLAN ID equals to**—Select the VLAN ID for the router ports that are described.
- **IP Version equals to**—Select the IP version that the Multicast router supports.
- **Interface Type equals to**—Select whether to display ports or LAGs.

STEP 3 Click **Go**. The interfaces matching the query criteria are displayed.

STEP 4 For each interface, select its association type. The options are as follows:

- *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 the dynamic learning of Multicast router ports, go to the **Multicast > IGMP Snooping Page,** and the **Multicast** > **MLD Snooping Page**
- *Forbidden*—This port is not to be configured as a Multicast router port, even if IGMP or MLD queries are received on this port. If **Auto Detect Mrouter Ports** is enabled on this port, the configuration does not succeed.
- *None*—The port is not currently a Multicast router port.

STEP 5 Click **Apply** to update the switch.

Defining Forward All Multicast

The *Forward All Page* enables and displays the configuration of the ports and/or LAGs that are to receive all of the Multicast stream from a specific VLAN. This feature requires that the Bridge Multicast filtering in the *Properties Page* be enabled. If it is disabled, then all Multicast traffic is flooded to all ports in the switch.

You can statically configure a port to Forward All, if the devices connecting to the port does not support IGMP and/or MLD.

IGMP or MLD messages are not forwarded to the ports are defined as *Forward All*.

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**. The *Forward All Page* opens.

STEP 2 Define the following:

- **VLAN ID equals to**—The VLAN ID the ports/LAGs are to be displayed.
- **Interface Type equals to**—Define whether to display ports or LAGs.

STEP 3 Click **Go**. The status of all ports/LAGs are displayed.

STEP 4 Select the interface that is to be defined as forward all by using the following methods:

- *Static*—The port receives all Multicast streams.
- *Dynamic*—Not applicable.
- *Forbidden*—Ports cannot receive any 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 5 Click **Apply**. The switch is updated.

Defining Unregistered Multicast Settings

Multicast frames are generally forwarded to all ports in the VLAN. If IGMP/MLD Snooping is enabled, the switch learns about the existence of Multicast groups, and monitors which ports have joined which Multicast group. Multicast groups can also be statically configured. Multicast groups that were either dynamically learned or statically configured, are considered registered. This enables the switch to forward the Multicast frames (from a registered Multicast group) only to ports that are joined to that Multicast group. The switch forwards Multicast frames (from a registered Multicast group) only to ports that are registered to that Multicast group.

The *Unregistered Multicast Page* enables handling Multicast frames that belong to groups that are not known to the switch (unregistered Multicast groups). Unregistered Multicast frames are usually forwarded to all ports on the VLAN.

You can select a port to receive or filter unregistered Multicast streams. The configuration is valid for any VLAN of which it is a member (or will be a member).

This feature ensures that the customer receives only the Multicast groups requested and not others that may be transmitted in the network.

To define unregistered Multicast settings:

STEP 1 Click **Multicast** > **Unregistered Multicast**. The *Unregistered Multicast Page* opens.

STEP 2 Define the following:

- **Interface Type equals to**—The view as all ports or all LAGs.
- **Entry No.**—The entry number in the Unregistered Multicast Table.
- **Interface**—Displays the interface ID.
- **Unregistered Multicast**—Displays the forwarding status of the selected interface. The possible values are:
  - *Forwarding*—Enables forwarding of unregistered Multicast frames to the selected interface.
  - *Filtering*—Enables filtering (rejecting) of unregistered Multicast frames to the selected interface.

STEP 3 Click **Edit**. The *Edit Unregistered Multicast Page* opens.

STEP 4 Define the Unregistered Multicast field.

- **Interface**—Select the interface to be modified.
- **LAG**—Select the LAG to be modified.
- **Unregistered Multicast**—Define the forwarding status of the interface. The options are as follows:
  - *Forwarding*—Enables forwarding of unregistered Multicast frames to the selected interface.
  - *Filtering*—Enables filtering of unregistered Multicast frames to the selected interface.

STEP 5 Click **Apply**. The settings are saved, and the switch is updated.

15

Configuring IP Information

IP interface addresses are configured manually by the user, or auto-configured by a DHCP server. This chapter provides information for defining the switch IP addresses.

It includes the following topics:

- **Management and IP Interfaces**
- **Configuring ARP**
- **Domain Name Systems**

Management and IP Interfaces

IP Addressing

The factory default setting of the IP address configuration is *DHCP*. This means that the switch acts as a DHCP client, and sends out a DHCP request during boot up.

If the switch receives a DHCP response from the DHCP server with an IP address, it sends Address Resolution Protocol (ARP) packets to confirm that the IP address is unique. If the ARP response shows that the IP 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 DHCP response in 60 seconds, it continues to send DHCPDISCOVER queries, and adopts the default IP 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 IP addresses, the switch issues DHCP requests until it is assigned an IP address from a DHCP server. The management VLAN can be configured with a static or dynamic IP address. The IP subnets to which these IP addresses belong are known as directly connected/attached IP subnets.

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

- Unless the switch is configured with a static IP address, it issues DHCP queries until a response is received from a DHCP server.
- If the IP address on the switch is changed, the switch issues gratuitous ARP packets to the corresponding VLAN to check IP address collisions. This rule also applies when the switch reverts to the default IP address.
- The system status LED 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 status LED also changes to solid green. The 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.
- When no statically defined or DHCP-acquired IP address is available, the default IP address is used. When the other IP addresses becomes available, the addresses are automatically used. The default IP address is always on the management VLAN.

The Internet Protocol version 6 (IPv6) is a network-layer protocol for packet-switched internetworks. IPv6 was designed to replace IPv4, the predominantly deployed Internet protocol.

IPv6 introduces greater flexibility in assigning IP addresses because the address size increases from 32-bit to 128-bit addresses. IPv6 addresses are written as eight groups of four hexadecimal digits, for example FE80:0000:0000:0000:0000:9C00:876A:130B. The abbreviated form, in which a group of zeroes can be left out, and replaced with '::', is also acceptable, for example, ::-FE80::9C00:876A:130B.

IPv6 nodes require an intermediary mapping mechanism to communicate with other IPv6 nodes over an IPv4-only network. This mechanism, called a tunnel, enables IPv6-only hosts to reach IPv4 services, and allows isolated IPv6 hosts and networks to reach an IPv6 node over the IPv4 infrastructure.

The tunneling mechanism uses the ISATAP mechanism. This protocol treats the IPv4 network as a virtual IPv6 local link, with mappings from each IPv4 address to a link local IPv6 address.

The switch detects IPv6 frames by the IPv6 Ethertype.

IP Addressing

The switch operates as a Layer 2 VLAN-aware switch, and has no routing capabilities. The 200 Series switches do not have layer 3 capabilities.

IP Addressing

The switch has a single IP address in the management VLAN. This IP address and the default gateway can be configured with a static IP address, or by DHCP. The static IP address and default gateway are configured on the *IPv4 Interface Page*. The switch uses the default gateway, if configured, to communicate with devices that are not in the same IP subnet as 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.

NOTE All the IP addresses configured or assigned to the switch are also referred as Management IP addresses in this guide.

Defining an IPv4 Interface

To manage the switch by using the web-based switch configuration utility, the IPv4 switch 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 switch IP address:

STEP 1 Click **Administration** > **Management Interface** > **IPv4 Interface**. The *IPv4 Interface Page* opens.

STEP 2 Enter the values for the following fields:

- **Management VLAN**—Select the Management VLAN used to access the switch through telnet or the Web GUI. VLAN1 is the default Management VLAN.
- **IP Address Type**—Select one of the following options:
  - **Dynamic**—Discover the IP address using DHCP from the management VLAN.

- **Static**—Manually define a static IP address.

If a static IP address is used, configure the following fields.

- **IP Address**—Enter the IP address, and configure one of the following fields:
- **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 and 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 status.

  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, select those of the following fields that are enabled:

- **Auto Configuration via DHCP**—Displays status of auto-configuration feature. You can configure DHCP Auto Configuration from *Administration* > *File Management* > *DHCP Auto Configuration*.

STEP 3 Click **Apply**. The IPv4 interface settings are defined, and the switch is updated.

Defining IPv6 Global Configuration

The *IPv6 Global Configuration Page* defines the frequency of the IPv6 ICMP error messages generated by the switch.

To define IPv6 global parameters:

STEP 1 Click **Administration** > **Management Interface** > **IPv6 Global Configuration**.

The *IPv6 Global Configuration Page* opens.

STEP 2 Enter the values for the following fields:

- **ICMPv6 Rate Limit Interval**—Enter the time limit.
- **ICMPv6 Rate Limit Bucket Size**—Enter the maximum number of ICMP error message that can be sent by the switch per interval.

STEP 3 Click **Apply**. The IPv6 global parameters are defined, and the switch is updated.

Defining an IPv6 Interface

The *IPv6 Interfaces Page* displays the switch's IPv6 interface parameters and *enables* configuring this interface. An IPv6 interface can be configured on a port, a LAG, VLAN, or ISATAP tunnel interface. The switch supports one IPv6 interface as an IPv6 end device.

A tunnel interface is configured with an IPv6 address based on the settings defined in the *IPv6 Tunnel Page*.

To configure IPv6 interfaces:

STEP 1 Click **Administration** > **Management Interface** > **IPv6 Interfaces**.

The *IPv6 Interfaces Page* opens.

This page displays the IPv6 interfaces already configured.

STEP 2 Click **Add** to add a new IPv6 interface, that is to define on which interface IPv6 is enabled. The *Add IPv6 Interface Page* opens.

STEP 3 Enter the values.

- **IPv6 Interface**—Select a specific port, LAG, VLAN, or ISATAP tunnel.
- **Number of DAD Attempts**—Enter the number of consecutive neighbor solicitation messages that are sent while Duplicate Address Detection (DAD) is performed on the interface's Unicast IPv6 addresses. DAD verifies the uniqueness of new Unicast IPv6 addresses before the addresses are assigned. New addresses remain in a tentative state during DAD verification. Entering **0** in this field disables duplicate address detection processing on the specified interface. Entering **1** in this field indicates a single transmission without follow-up transmissions.
- **IPv6 Address Auto Configuration**— If enabled, the switch supports IPv6 stateless address auto configuration of site local and global IP address from the IPv6 router advertisement received on the interface. The switch does not support stateful address auto configuration.
- **Send ICMPv6 Messages**—Enable generating unreachable destination messages.

STEP 4 Click **Apply** to enable IPv6 processing on the selected interface. Regular IPv6 interfaces have the following addresses automatically configured:

- Link local address using EUI-64 format interface ID based on a device's MAC address
- All node link local Multicast addresses (FF02::1)
- Solicited-Node Multicast address (format FF02::1:FFXX:XXXX)

STEP 5 Click **IPv6 Address Table** to manually assign IPv6 addresses to the interface, if required. This page is described in the **"Defining IPv6 Addresses"** section.

Defining IPv6 Addresses

To assign an IPv6 address to an IPv6 Interface:

STEP 1 Click **Administration** > **Management Interface** > **IPv6 Addresses**.

The *IPv6 Address Page* opens.

STEP 2 Select an interface, and click **Go**. The interface is displayed in the IPv6 Address Table.

STEP 3 Click **Add**. The Add IPv6 Address Page opens.

STEP 4 Enter the values for the fields.

- **IPv6 Interface**—Displays the interface where the address is automatically completed, based on the filter.
- **IPv6 Address Type**—Select Link Local or Global as the type of IPv6 address to add.
  - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- **IPv6 Address**—The switch supports one IPv6 interface. In additional to the default link local and Multicast addresses, the device also automatically adds global addresses to the interface based on the router advertisements

it receives. The device supports a maximum of 128 addresses at the interface. Each address must be a valid IPv6 address that is specified in hexadecimal format by using 16-bit values separated by colons.

NOTE You cannot configure any IPv6 addresses directly on a ISATAP tunnel interface.

- **Prefix Length**—The length of the Global IPv6 prefix as a decimal value from 0-128 indicating the number of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
- **EUI-64**—Select to use the EUI-64 parameter to identify the interface ID portion of the Global IPv6 address by using the EUI-64 format based on a device MAC address.

STEP 5 Click **Apply**. The switch is updated.

Viewing the IPv6 Default Router List

The *IPv6 Default Router List Page* enables configuring and viewing the default IPv6 router addresses. This list contains 0 or more routers that are candidates to become the switch default router for non-local traffic. The switch randomly selects a router from the list. The switch supports one static IPv6 default router. Dynamic default routers are routers that have sent router advertisements to the switch IPv6 interface.

When adding or deleting IP addresses, the following events occur:

- When removing an IP interface, all the default router IP addresses are removed.
- Dynamic IP addresses cannot be removed.
- An alert message is displayed after an attempt is made to insert more than a single user-defined address.
- An alert message is displayed when attempting to insert a non-link local type address, meaning 'fe80:'.

To define a default router:

STEP 1 Click **Administration** > **Management Interface** > **IPv6 Default Router List**.

The *IPv6 Default Router List Page* opens.

This page displays the following fields for each default router:

- **Default Router IPv6 Address**—Link local IP address of the default router.
- **Interface**—Outgoing IPv6 interface where the default router resides.
- **Type**—The default router configuration that includes the following options:
  - *Static*—The default router was manually added to this table through the **Add** button.
  - *Dynamic*—The default router was dynamically configured.

  State—The default router status options are:
  - *Incomplete*—Address resolution is in process. Default router has not yet responded.
  - *Reachable*—Positive confirmation was received within the Reachable Time.
  - *Stale*—Previously-known neighboring network is unreachable, and no action is taken to verify its reachability until it is necessary to send traffic.
  - *Delay*—Previously-known neighboring network is unreachable. The switch is in Delay state for a predefined *Delay Time.* If no confirmation is received, the state changes to Probe.
  - *Probe*—Neighboring network is unavailable, and Unicast Neighbor Solicitation probes are being sent to verify the status.

STEP 2 Click **Add** to add a static default router. The *Add Default Router Page* opens.

The window displays the Link Local Interface. The interface can be a port, LAG, VLAN, or tunnel.

STEP 3 Enter the static default router IP address in the Default Router IPv6 Address field.

STEP 4 Click **Apply**. The default router is defined, and the switch is updated.

Configuring IPv6 Tunnels

The ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) enables encapsulating IPv6 packets within IPv4 packets for transmission over IPv4 networks. You must first manually enable and configure an ISATAP tunnel. Then you manually define an IPv6 interface at the ISATAP tunnel. Then the switch automatically configures the link local IPv6 address to the IPv6 interface.

When defining ISATAP tunnels, note the following:

- An IPv6 link local address is assigned to the ISATAP interface. The initial IP address is assigned to the interface, which is then activated.
- If an ISATAP interface is active, the ISATAP router IPv4 address is resolved via DNS by using ISATAP-to-IPv4 mapping. If the ISATAP DNS record is not resolved, ISATAP host name-to-address mapping is searched in the host mapping table.
- When the ISATAP router IPv4 address is not resolved via the DNS process, the ISATAP IP interface remains active. The system does not have a default router for ISATAP traffic until the DNS process is resolved.

To configure an IPv6 Tunnel:

STEP 1 Click **Administration** > **Management Interface** > **IPv6 Tunnel**.

The *IPv6 Tunnel Page* opens.

STEP 2 Enter the values for the following fields:

- **Tunnel Number**—Displays the automatic tunnel router domain number.
- **Tunnel Type**—Always displayed as ISATAP.
- **Source IPv4 Address**—Disable the ISATAP tunnel, or enable the ISATAP tunnel over an IPv4 interface. The IPv4 address of the selected IPv4 interface used to form part of the IPv6 address over the ISATAP tunnel interface. The IPv6 address has a 64-bit network prefix of fe80::, with the rest of the 64-bit formed by concatenating 0000:5EFE and the IPv4 address.
  - *Auto*—Automatically selects the lowest IPv4 address from among all of its configured IPv4 interfaces.
  - *None*—Disable the ISATAP tunnel.
  - *Manual*—Manually configure an IPv4 address. The IPv4 address configured must be one of the IPv4 addresses at the switch IPv4 interfaces.

- **Tunnel Router's Domain Name**—A global string that represents a specific automatic tunnel router domain name. The name can either be the default name (ISATAP) or a user defined name.
- **Query Interval**—The number of seconds from 10-3600 between DNS queries (before the IP address of the ISATAP router is known) for this tunnel. The interval can be the default value (10 seconds) or a user defined interval.
- **ISATAP Solicitation Interval**—The number of seconds from 10-3600 between ISATAP router solicitations messages, when there is no active ISATAP router. The interval can be the default value (10 seconds) or a user defined interval.
- **ISATAP Robustness**—Used to calculate the interval for the DNS or router solicitation queries. The bigger the number, the more frequent the queries. The default value is 3. The range is 1-20.

  NOTE The ISATAP tunnel is not operational if the underlying IPv4 interface is not in operation.

STEP 3 Click **Apply**. The tunnel is defined, and the switch is updated.

Defining IPv6 Neighbors Information

The *IPv6 Neighbors Page* enables configuring and viewing the list of IPv6 neighbors on the IPv6 interface. The IPv6 Neighbor Table (also known as IPv6 Neighbor Discovery Cache) displays the MAC addresses of the IPv6 neighbors that are in the same IPv6 subnet as the switch. This is used to verify the reachability of this neighbor. This is the IPv6 equivalent of the IPv4 ARP Table. When the switch needs to communicate with its neighbors, the switch uses the IPv6 Neighbor Table to determine the MAC addresses based on their the IPv6 addresses.

This page displays the neighbors that were automatically detected or manually configured entries. Each entry displays to which interface the neighbor is connected, the neighbor's IPv6 and MAC addresses, the entry type (static or dynamic), and the state of the neighbor.

To define IPv6 neighbors:

STEP 1 Click **Administration** > **Management Interface** > **IPv6 Neighbors**

The *IPv6 Neighbors Page* opens.

STEP 2 Select a **Clear Table** option to clear some or all of IPv6 addresses in the IPv6 Neighbors Table.

- *Static Only*—Deletes the static IPv6 address entries.
- *Dynamic Only*—Deletes the dynamic IPv6 address entries.
- *All Dynamic & Static*—Deletes the static and dynamic address entries IPv6 address entries.

The following fields are displayed for the neighboring interfaces:

- **Interface**—Neighboring IPv6 interface type.
- **IPv6 Address**—IPv6 address of a neighbor.
- **MAC Address**—MAC address mapped to the specified IPv6 address.
- **Type**—Neighbor discovery cache information entry type (static or dynamic).
- **State**—Specifies the IPv6 neighbor status. The values are:
  - *Incomplete*—Address resolution is working. The neighbor has not yet responded.
  - *Reachable*—Neighbor is known to be reachable.
  - *Stale*—Previously-known neighbor is unreachable. No action is taken to verify its reachability until traffic must be sent.
  - *Delay*—Previously-known neighbor is unreachable. The interface is in Delay state for a predefined Delay Time. If no reachability confirmation is received, the state changes to Probe.
  - *Probe*—Neighbor is no longer known to be reachable, and Unicast Neighbor Solicitation probes are being sent to verify the reachability.

STEP 3 Click **Add**. The *Add IPv6 Neighbors Page* opens.

The *Add IPv6 Neighbors Page* provides information for adding a neighbor to be monitored.

STEP 4 Enter the values for the following fields:

- **Interface**—The neighboring IPv6 interface to be added.
- **IPv6 Address**—Enter the IPv6 network address assigned to the interface. The address must be a valid IPv6 address.
- **MAC Address**—Enter the MAC address mapped to the specified IPv6 address.

STEP 5 Click **Apply**. The switch is updated.

Modifying an IPv6 Neighbor

To modify an IPv6 Neighbor:

STEP 1 Click **Administration** > **Management Interface** > **IPv6 Neighbors**

The *IPv6 Neighbors Page* opens.

STEP 2 Select an interface, and click **Edit.** The *Edit IPv6 Neighbors Page* opens.

STEP 3 Enter the values for the following fields:

- **IPv6 Address**—Select a valid IPv6 address.
- **MAC Address**—Select the MAC address mapped to the specified IPv6 address.
- **Type**—Select the type of the neighbor discovery cache information entry.
  - *Static*—The static neighbor discovery cache entries.
  - *Dynamic*—The dynamic neighbor discovery cache entries.

STEP 4 Click **Apply**. The switch is updated.

Viewing IPv6 Route Tables

The *IPv6 Routes Table Page* displays the IPv6 Routes Table. The table contains a single default route (IPv6 address::0) that uses the default router selected from the IPv6 Default Router List to send packets to destination devices that are not in the same IPv6 subnet as the switch. In addition to the default route, the table also contains dynamic routes which are ICMP redirect routes received from IPv6 routers by using ICMP redirect messages. This could happen when the default router the switch uses is not the router for traffic to the IPv6 subnets that the switch wants to communicate to.

To view IPv6 routing entries, click **Administration** > **Management Interface** > **IPv6 Routes**.

The *IPv6 Routes Table Page* opens.

This page displays the following fields:

- **IPv6 Address**—The IPv6 subnet address.
- **Prefix Length**—IP route prefix length for the destination IPv6 subnet address. It is preceded by a forward slash.
- **Interface**—Interface used to forward the packet.
- **Next Hop**—Address where the packet is forwarded. Typically, this is the address of a neighboring router. This must be a link local address.
- **Metric**—Value used for comparing this route to other routes with the same destination in the IPv6 router table. All default routes have the same value.
- **Life Time**—Time period that the packet can be sent, and resent, before being deleted.
- **Route Type**—How the destination is attached, and the method used to obtain the entry. The following values are:
  - *Local*—The manually configured switch IPv6 address.
  - *Dynamic*—The destination is indirectly attached IPv6 subnet address. The entry was obtained dynamically via the ICMP protocol.

Configuring ARP

The switch maintains an ARP (Address Resolution Protocol) Table for all the known devices that reside in its directly connected IP subnets. A directly connected IP subnet is the subnet that a IPv4 interface of the switch is connected to. When the switch needs to send/route a packet to a local device, it searches the ARP Table to obtain the MAC address of the device. The ARP Table contains both static and dynamic addresses. Static addresses are manually configured and do not age out. The switch creates dynamic addresses from the ARP packets it receives. Dynamic addresses age out after a configured time.

The *ARP Table Page* enables viewing dynamic ARP entries that the switch has learned, changing the ARP entry aging time, clearing ARP entries, and adding or deleting static ARP entries.

NOTE The IP/MAC address mapping information in the ARP Table is used by the switch to forward traffic originated by the switch.

To define the ARP tables:

STEP 1 Click **IP Configuration** > **ARP**. The *ARP Table Page* opens.

STEP 2 Enter the parameters.

- **ARP Entry Age Out**—Enter the number of seconds that dynamic addresses can remain in the ARP Table. A dynamic address ages out after the time it is in the table exceeds the ARP Entry Age Out time. When a dynamic address ages out, it is deleted from the table, and needs to be relearned to be entered into the table again.
- **Clear ARP Table Entries**—Select the type of ARP entries to be cleared the system.
  - *All*—Deletes all of the static and dynamic addresses immediately.
  - *Dynamic*—Deletes all of the dynamic addresses immediately.
  - *Static*—Deletes all of the static addresses immediately.
  - *Normal Age Out*—Deletes dynamic addresses based on the configured ARP Entry Age Out time.

The ARP Table displays the following fields:

- **Interface**—The IPv4 Interface of the directly connected IP subnet where the IP device resides.

- **IP Address**—The IP address of the IP device.
- **MAC Address**—The MAC address of the IP device.
- **Status**—Whether the entry was manually entered or dynamically learned.

STEP 3 Click **Apply.** The ARP global settings are modified, and the switch is updated.

STEP 4 Click **Add**. The *Add ARP Page (Layer 2)* opens.

STEP 5 Enter the parameters.

- **IP Version**—The IP address format supported by the host. Only IPv4 is supported.
- **Interface**—IPv4 interface on the switch.

There is only one directly connected IP subnet, which is always in the management VLAN. All the static and dynamic addresses in the ARP Table reside in the management VLAN.

- **IP Address**—Enter the IP address of the local device.
- **MAC Address**—Enter the MAC address of the local device.

STEP 6 Click **Apply**. The ARP entry is defined, and the switch is updated.

Domain Name Systems

The Domain Name System (DNS) translates user-defined domain names into IP addresses for the purpose of locating and addressing these objects.

As a DNS client the switch resolves domain names to IP addresses through one or more configured DNS servers.

Defining DNS Servers

The *DNS Servers Page* enables configuring the DNS servers and the default domain used by the switch.

To configure DNS servers:

STEP 1 Click **IP Configuration** > **Domain Name System** > **DNS Servers**. The *DNS Servers Page* opens.

STEP 2 Enter the parameters.

- **DNS**—Select to enable the switch as a DNS client to resolve DNS names into IP addresses through one or more configured DNS servers.
- **Default Domain Name**—Enter the default DNS domain name (1–158 characters). The switch appends to all non-fully qualified domain names (FQDN) turning them into FQDNs.
- **Type**—Displays the default domain type options:
  - *DHCP*—The default domain name is dynamically assigned by the DHCP server.
  - *Static*—The default domain name is user-defined.
  - N/A—No default domain name.

DNS Server Table:

- **DNS Server**—The IP addresses of the DNS servers. Up to eight DNS servers can be defined.
- **Server State**—The active DNS server. There can be only one active server. Each static server has a priority, a lower value means a higher priority. When first time the request is sent, static server with lowest priority is chosen. If after two retries there is no response from this server, the next server with the next lowest priority is selected. If none of the static servers respond, the first dynamic server on the table, sorted by IP address (low to high), is selected.

STEP 3 Click **Add.** The *Add DNS Server Page* opens.

STEP 4 Enter the parameters.

- **IP Version**—Select Version 6 for IPv6 or Version 4 for IPv4.

- **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are:
  - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- **Link Local Interface**—If the IPv6 address type is Link Local, select whether it is received through VLAN2 or ISATAP.
- **DNS Server IP Address**—Enter the DNS server IP address.
- **Set DNS Server Active**—Select to activate the new DNS server.

STEP 5 Click **Apply**. The DNS server is added, and the switch is updated.

Mapping DNS Hosts

The switch saves the frequently-queried domain names acquired from the DNS servers into the local DNS cache. The cache can hold up to 64 static entries, 64 dynamic entries, and one entry for each IP address configured on the switch by DHCP. Name resolution always begins by checking these static entries, continues by checking the local DNS cache, and ends by sending requests to the external DNS server.

The *Host Mapping Page* enables configure static mappings between a DNS host name and an IP address.

Several IP addresses are supported per DNS per host name.

To add a domain name and its IP address:

STEP 1 Click **IP Configuration** > **Domain Name System** > **Host Mapping**. The *Host Mapping Page* opens.

This page displays the following fields:

- **Host Name**—User-defined domain name, up to 158 characters.
- **IP Address**—The host name IP address.

STEP 2 Click **Add**. The *Add Host Mapping Page* opens.

STEP 3 Enter the parameters.

- **IP Version**—Select Version 6 for IPv6 or Version 4 for IPv4.
- **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are:
  - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- **Link Local Interface**—If the IPv6 address type is Link Local, select whether it is received through VLAN2 or ISATAP.
- **Host Name**—Enter a domain name, up to 158 characters.
- **IP Address**—Enter an IP v4 IP address or enter up to four IPv6 host IP addresses. Addresses 2–4 are backup addresses.

STEP 4 Click **Apply**. The DNS host is added, and the switch is updated.

16

Configuring Security

This chapter describes various aspects of security and access control. The system handles various types of security. Some features are used for more than a single type of security or control, and so they appear twice in the list of topics below. The following list of topics describes the various types of security features described in this chapter:

Permission to administer the switch is detailed in the following sections:

- **Defining Users**
- **Configuring RADIUS Parameters**
- **Configuring Management Access Authentication**
- **Defining Access Profiles**
- **Configuring TCP/UDP Services**

Protection from attacks directed at the switch CPU is detailed in the following sections:

- **Configuring TCP/UDP Services**
- **Defining Storm Control**

Access control of end-users to the network through the switch is detailed in the following sections:

- **Configuring Management Access Authentication**
- **Defining Access Profiles**
- **Defining Users**
- **Configuring RADIUS Parameters**
- **Configuring Port Security**
- **Configuring 802.1X**

Protection from other network users is detailed in the following sections. These are attacks that pass through, but are not directed at, the switch.

- **Configuring TCP/UDP Services**
- **Defining Storm Control**
- **Configuring Port Security**

Defining Users

A user, in this context, is a system administrator or superuser, who manages the switch.

The default username is **cisco** and the default password is **cisco**. The first time that you log in with the default username and password, you are required to enter a new password. If the password that you choose is not complex enough, you will be prompted to create another password.

Setting User Accounts

The *User Accounts Page* enables entering additional users that are permitted to manage the switch or changing the passwords of existing users.

NOTE It is not permitted to delete all users. If all users are selected, the **Delete** button is disabled.

To add a new user:

STEP 1 Click **Administration** > **User Accounts**. The *User Accounts Page* displays.

This page displays the users defined in the system.

STEP 2 Click **Add** to add a new user or click **Edit** to modify a user. The *Add (or Edit) a User Account Page* displays.

STEP 3 Enter the parameters.

- **User Name**—Enter a new username between 0 and 20 characters. UTF-8 characters are not permitted.

- **Password**—Enter a password (UTF-8 characters are not permitted). If the password strength and complexity is defined, the user password must comply with the policy. This is configured in the **Setting Password Complexity Rules** section.
- **Confirm Password**—Enter the password again.
- **Password Strength Meter**—Displays the strength of password. The policy for password strength and complexity are configured in the *Password Strength Page*.

STEP 4 Click **Apply**. The user is added, and the switch is updated.

Setting Password Complexity Rules

Passwords are used to authenticate users accessing the switch. Password management consists of setting general password complexity rules and the specific user passwords. Various aspects of password complexity are minimum password length, number of character classes, and the requirement that a new password be different from the previous one.

The *Password Strength Page* enables setting password complexity, as well as aging (the length of time during which the password is valid).

To define password complexity rules:

STEP 1 Click **Security** > **Password Strength**. The *Password Strength Page* displays.

STEP 2 Clear **Password Complexity Settings** to turn off the definition of complexity rules for passwords.

STEP 3 Enter the parameters.

- **Minimal Password Length**—Enter the minimal number of characters required for passwords.
- **Minimal Number of Character Classes**—Enter the character classes that must comprise a password: lower case letters (1), upper case letters (2), digits (3), or special characters (4).
- **The New Password Must Be Different than the Current One**—If selected, the new password cannot be the same as the current password.
- **Password Aging**—If selected, the user is prompted to change the password when the **Password Aging Time** expires.

- **Password Aging Time**—Enter the number of days that can elapse before the user must change the password. The default is 180 days.

STEP 4 Click **Apply**. The password settings are set, and the switch is updated.

Configuring RADIUS Parameters

Remote Authorization Dial-In User Service (RADIUS) servers provide a centralized 802.1X or MAC-based network access control. The switch is a RADIUS client that relies on a RADIUS server to provide centralized security, authorizing and authenticating users attempting to access and administer the switch.

For the RADIUS server to grant access to the web-based switch configuration utility, the RADIUS server must return cisco-avpair = shell:priv-lvl=15.

Use this page to enable the configuration of the RADIUS server parameters the switch uses to communicate with the servers.

To set the default RADIUS parameters:

STEP 1 Click **Security** > **RADIUS**. The *RADIUS Page* displays.

The RADIUS table displays the specific parameters for each defined RADIUS server.

STEP 2 Enter the default RADIUS parameters. Values entered in the *Default Parameters* are applied to all servers. If a value is not entered for a specific server the switch uses the values in these fields.

- **IP Version**—Displays the supported IP version: IPv6 and/or IPv4 subnet.
- **Number of 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.
- **Dead Time**—Enter the number of minutes that elapse before a non-responsive RADIUS server is bypassed for service requests. If the value is 0, the server is not bypassed.

- **Key String**—Enter the default key string used for authenticating and encrypting the RADIUS attributes communicated between the switch and the RADIUS server. This key must match the key configured on the RADIUS server. A key string is used to encrypt communications by using MD5. A key configured for an individual RADIUS server has precedence over the default key that is used if there is no key provided for an individual server.

STEP 3 Click **Apply**. The RADIUS settings for the switch are updated.

To add a RADIUS Server:

STEP 1 Click **Security** > **RADIUS**. The *RADIUS Page* displays.

STEP 2 Click **Add.** The *Add RADIUS Server Page* displays.

This page provides fields that must be entered individually for a server.

STEP 3 Enter the values in the fields for each server. To use the default values entered in the *RADIUS Page*, select **Use Default**.

- **Server Definition**—Select whether to specify the RADIUS server by IP address or name.
- **IP Version**—If the RADIUS server will be identified by IP address, select either IPv4 or IPv6, to indicate that it will be entered in the selected format.
- **Server IP Address/Name**—Address or host name of the RADIUS server. Whether this is an IP address or host name depends on the Server Definition.
- **Priority**—Enter the priority of the server. The priority determines the order the switch attempts to contact the servers to authenticate a user. The switch will start with the highest priority RADIUS server first. Zero is the highest priority.
- **Key String**—Enter the key string used for authenticating and encrypting the RADIUS attributes communicated between the switch and the RADIUS server. This key must match the key configured on the individual RADIUS server. If this field is left blank, the switch attempts to authenticate to the RADIUS server by using the default Key String.
- **Timeout for Reply**—Enter the number of seconds the switch waits for an answer from the RADIUS server before retrying the query, or switching to the next server. If there is no value entered in this field, the switch uses the default timeout value.

- **Authentication Port**—Enter the UDP port number of the RADUS server for authentication requests.
- **Accounting Port**—Enter the UDP port number of the RADUS server for accounting requests.
- **Number of Retries**—Enter the number of requests that are sent to the RADIUS server before a failure is considered to have occurred. Select **Use Default** to use the default value for the number of retries.
- **Dead Time**—Enter the number of minutes that must pass before a non-responsive RADIUS server is bypassed for service requests. Select **Use Default** to use the default value for the dead time. If you enter 0 minutes, there is no dead time.
- **Usage Type**—Enter the RADIUS server authentication type. The options are:
  - *Login*—RADIUS server is used for authenticating users that 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 4 Click **Apply**. The RADIUS server is added, and the switch is updated.

Configuring Management Access Authentication

Authentication methods can be assigned to HTTP sessions. This authentication can be performed locally or on an external RADIUS server.

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; 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**. The *Management Access Authentication Page* displays.

STEP 2 Select an access method from the **Application** list.

STEP 3 Use the arrows to move the authentication method between the Optional Methods column and the Selected Methods column. The first method selected is the first method that is used.

- *RADIUS*—User is authenticated on a RADIUS server. You must have configured one or more RADIUS servers.
- *None*—User is allowed to access the switch without authentication.
- *Local*—Username and password is checked against the data stored on the local switch. These username and password pairs are defined in the *User Accounts Page*.

  NOTE The **Local** or **None** authentication method must always be selected last. All authentication methods selected after **Local** or **None** are ignored.

STEP 4 Click **Apply**. The selected authentication methods are associated with the access method.

Defining Access Profiles

Management Access Authentication configures the authentication methods to be used to authenticate and authorize users from different management access methods. Management Access Profiles limit management access from specific interfaces and/or sources.

Only users who pass both the active access profile and management access authentication are given management access to the switch.

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**—The HTTP access method is available.
- **Action**—Permit or deny access to an interface or source address.
- **Interface**—Which ports, LAGs, or VLANs are permitted to access or denied access to the web-based switch configuration utility.
- **Source IP Address**—IP addresses or subnets that are allowed access.

Active Access Profile

The *Access Profiles Page* displays the active access profile and all access profiles created by users. 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.

The lookup in the active access profile is done by using a first-match method. The switch looks to see if the active access profile explicitly permits management access to the switch. If no match is found, access is denied.

When an attempt to access the switch is in violation of the active access profile, the switch generates a SYSLOG message to alert the system administrator of the attempt.

After an access profile has been defined, additional rules can be added or edited by using the *Profiles Rules Page*.

Displaying, Adding, or Activating an Access Profile

To display, add, or select a different active access profile:

STEP 1 Click **Security** > **Mgmt Access Method** > **Access Profiles**. The *Access Profiles Page* displays.

This page displays all of the access profiles, active and inactive.

STEP 2 To change the active access profile, select a profile from the **Active Access Profile** drop down menu and click **Apply**. This makes the chosen profile the active access profile.

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

NOTE Some 200 Series switches only support web access (http only, not https). The profile you define may be customized according to a set of settings provided in Access Profile entry, but ultimately will only provide web access; console or any other methods (HTTPS, SSH & Telnet) are not supported.

STEP 3 Click **OK** to select the active access profile or click **Cancel** to discontinue the action.

STEP 4 Click **Add** to open the *Add Access Profile Page*. The page allows you to configure a new profile and one rule. Go to the **Defining Profile Rules** section for instructions on how to construct a rule.

STEP 5 Enter the parameters.

- **Access Profile Name**—Enter an access profile name. The access profile name can contain up to 32 characters.
- **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**— HTTP management is available.
- **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 only to the port, or LAG selected.
- **Applies to Source IP Address**—Select the type of source IP address to which the access profile applies. The *Source IP Address* field is valid for a subnetwork. Select one of the following values:
  - *All*—Applies to all types of IP addresses.

- *User Defined*—Applies to only those types of IP addresses defined in the fields.

- **IP Version**—Select the supported IP version of the source address, IPv6 or IPv4.
- **IP Address**—Enter the source IP address.
- **Mask**—Select the format for the subnet mask for the source IP address, and enter a value in one of the fields:
  - **Network Mask**—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
  - **Prefix Length**—Select the Prefix Length and enter the number of bits that comprise the source IP address prefix.

STEP 6 Click **Apply**. The access profile is created, and the switch is updated. You can now select this access profile as the active access profile.

Defining Profile Rules

Access profiles can contain up to 128 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 define profile rules:

STEP 1 Click **Security** > **Mgmt Access Method** > **Profile Rules**. The *Profiles Rules Page* displays.

STEP 2 Select the Filter field, and an access profile. Click **Go**.

The selected access profile is displayed in the Profile Rule Table.

STEP 3 Click **Add** to add a rule to it. The *Add Profile Rule Page* displays.

STEP 4 Enter the parameters.

- **Access Profile Name**—Select an access profile.
- **Rule Priority**—Enter the rule priority. When the packet is matched to a rule, user groups are either granted or denied access to the switch. The rule priority is essential to matching packets to rules, as packets are matched on a first-fit basis.
- **Management Method**—Displays the management method for which the rule is defined.
- **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 ports, VLANs, and LAGs.
  - *User Defined*—Applies only to the port, VLAN, or LAG selected.
- **Applies to Source IP Address**—Select the type of source IP address to which the access profile applies. The *Source IP Address* field is valid for a subnetwork. Select one of the following values:
  - *All*—Applies to all types of IP addresses.
  - *User Defined*—Applies to only those types of IP addresses defined in the fields.
- **IP Version**—Select the supported IP version of the source address: IPv6 or IPv4.
- **IP Address**—Enter the source IP address.
- **Mask**—Select the format for the subnet mask for the source IP address, and enter a value in one of the 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,** and the rule is added to the access profile.

Configuring TCP/UDP Services

The *TCP/UDP Services Page* enables TCP or UDP-based services on the switch, usually for security reasons.

The switch offers HTTP TCP/UDP services.

To view these services:

STEP 1 Click **Security** > **TCP/UDP Services**. The *TCP/UDP Services Page* displays.

The TCP Services table displays the following information:

- **HTTP Service**—Indicates whether HTTP service is enabled or disabled.
- **Service Name**—Management access method through which the switch is offering the service.
- **Type**—IP protocol 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**—Status of the service.

The UDP Services table displays the following information:

- **Service Name**—Management access method through which the switch is offering the service.
- **Type**—IP protocol the service uses.
- **Local IP Address**—Local IP address through which the switch is offering the service.
- **Local Port**—Local UDP port through which the switch is offering the service.

- **Application Instance**—The service instance of the UDP service. (For example, when two senders send to the same destination.)

Defining Storm Control

When Broadcast, Multicast, or Unknown Unicast frames are received, they are duplicated, and a copy is sent to all possible egress ports. This means that in practice they are sent to all ports belonging to the relevant VLAN. In this way, one ingress frame is turned into many, creating the potential for a 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 a threshold (limit) is entered in the system, the port discards traffic after that threshold is reached. The port remains blocked until the traffic rate drops below this threshold. It then resumes normal forwarding.

To define Storm Control:

STEP 1 Click **Security** > **Storm Control**. The *Storm Control Page* displays.

This page displays storm control parameters for all ports.

All the fields on this page are described in the *Edit Storm Control Page* except for the **Storm Control Rate Threshold (%)**. It displays the percent of the total available bandwidth for unknown Unicast, Multicast, and Broadcast packets before storm control is applied at the port. The default value is 10% of the maximum rate of the port and is set in the *Edit Storm Control Page*.

STEP 2 Select a port and click **Edit.** The *Edit Storm Control Page* displays.

STEP 3 Enter the parameters.

- **Port**—Select the port for which storm control is enabled.
- **Storm Control**—Select to enable Storm Control.
- **Storm Control Rate Threshold**—Enter the maximum rate at which unknown packets can be forwarded. The default for this threshold is 10,000 for FE devices and 100,000 for GE devices.

- **Storm Control Mode**—Select one of the modes:
  - *Unknown Unicast, Multicast & Broadcast*—Counts unknown Unicast, Broadcast, and Multicast traffic together towards the bandwidth threshold.
  - *Multicast & Broadcast*—Counts Broadcast and Multicast traffic together towards the bandwidth threshold.
  - *Broadcast Only*—Counts only Broadcast traffic towards the bandwidth threshold.

STEP 4 Click **Apply**. Storm control is modified, and the switch 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 port does not learn any new MAC addresses. The learned addresses are not subject to aging or re-learning.
- **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 re-learning.

When a frame from a new MAC address is detected on a port where it is not authorized (the port is classically locked, and there is a new MAC address, or the port is dynamically locked, and the maximum number of allowed addresses has been exceeded), the protection mechanism is invoked, and one of the following actions can take place:

- Frame is discarded
- Frame is forwarded

- Port is shut down

When the secure MAC address is seen on another port, the frame is forwarded, but the MAC address is not learned on that port.

In addition to one of these actions, you can also generate traps, and limit their frequency and number to avoid overloading the devices.

NOTE Traps on the 200 Series are syslog related traps, not SNMP.

NOTE If you want to use 802.1X on a port, it must be multiple host mode (see the *802.1x, Host and Session Authentication Page)*.

The *Port Security Page* displays security parameters for all ports and LAGs, and enables their modification.

To configure port security:

STEP 1 Click **Security** > **Port Security**. The *Port Security Page* displays.

This page displays information either for all ports or for all LAGs, depending on which interface type is selected.

STEP 2 Select an interface to be modified, and click **Edit.** The *Edit Port Security Interface Settings Page* displays.

STEP 3 Enter the parameters.

- **Interface**—Select the interface name.
- **Interface Status**—Select to lock the port.
- **Learning Mode**—Select the type of port locking. To configure this field, the Interface Status must be unlocked. The Learning Mode field is enabled only if the *Interface Status* field is locked. To change the Learning Mode, the Lock Interface must be cleared. After the mode is changed, the Lock Interface can be reinstated. The options are:
  - *Classic Lock*—Locks the port immediately, regardless of the number of addresses that have already been learned.
  - *Limited Dynamic Lock*—Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both 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 port if *Limited Dynamic Lock* learning mode is selected. The range is 0-256 and the default is 1. The number 0 indicates that only static addresses are supported on the interface.
- **Action on Violation**—Select an action to be applied to packets arriving on a locked port. The options are:
  - *Discard*—Discards packets from any unlearned source.
  - *Forward*—Forwards packets from an unknown source without learning the MAC address.
  - *Shutdown*—Discards packets from any unlearned source, and shuts down the port. The port remains shut down until reactivated, or until the switch is rebooted.
- **Trap**—Select to enable traps when a packet is received on a locked port. This is relevant for lock violations. For Classic Lock, this is any new address received. For Limited Dynamic Lock, this is any new address that exceeds the number of allowed addresses.

  NOTE Traps on the 200 Series are syslog related and not through SNMP. The 200 Series does not support SNMP.
- **Trap Frequency**—Enter minimum time (in seconds) that elapses between traps.

STEP 4 Click **Apply**. Port security is modified, and the switch 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 the 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 the supplicant permitted to send data to the port. Otherwise, the authenticator discards the supplicant data.

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**:
  - **A1**—Single-session/single host. In this mode, the switch, as an authenticator supports one 802.1x session and grants permission to use the port to the authorized supplicant at a port. All the access by the 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 unauthenticated 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 to a supplicant at the port.
- **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.

Authentication Methods

The authentication method can be:

- 802.1x—The switch supports the authentication mechanism as described in the standard to authenticate and authorize 802.1x supplicants.

802.1X Parameters Workflow

Define the 802.1X parameters as follows:

6. Define 802.1X settings for each port by using the *Edit Port Authentication Page*.
7. Define host authentication parameters for each port using the *Port Authentication Page*.
8. 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. For 802.1X to function, it must be activated both globally and individually on each port.

To define port-based authentication:

STEP 1 Click **Security** > **802.1X** > **Properties**. The *802.1X Properties Page* displays.

STEP 2 Enter the parameters.

- **Port Based Authentication**—Enable or disable port-based, 802.1X authentication.

STEP 3 Click **Apply**. The 802.1X properties are modified, and the switch is updated.

Defining 802.1X Port Authentication

The *Port Authentication Page* enables configuration of several of the 802.1X parameters for each port. Since some of the configuration changes are only possible while the port is in *Force Authorized* state, such as host authentication, it is recommended that you change the port control to *Force Authorized* before making changes. When the configuration is complete, return the port control to its previous state.

NOTE A port with 802.1x defined on it cannot become a member of a LAG.

To define 802.1X authentication:

Click **Security** > **802.1X** > **Port Authentication**. The *Port Authentication Page* displays.

This page displays authentication settings for all ports.

Modifying 802.1X Port Authentication Settings

STEP 1 Click **Security** > **802.1X** > **Port Authentication**. The *Port Authentication Page* displays.

STEP 2 Select a port, and click **Edit.** The *Edit Port Authentication Page* displays.

STEP 3 Enter the parameters.

- **Port**—Select a port.
- **User Name**—Displays the username of the port.
- **Current Port Control**—Displays the current port authorization state. If the state is *Authorized*, the port is either authenticated or the *Administrative Port Control* is *Force Authorized*. Conversely, if the state is *Unauthorized*, then the port is either not authenticated or the *Administrative Port Control* is *Force Unauthorized*.
- **Administrative Port Control**—Select the Administrative Port Authorization state. The options are:
  - *Force Unauthorized*—Denies the interface access by moving the interface into the unauthorized state. The 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.
- **Authentication Method**—*802.1X Only* method is available.
- **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. The options are:
  - *Force-Authorized*—Controlled port state is set to Force-Authorized (forward traffic).
  - *Force-Unauthorized*—Controlled port state is set to Force-Unauthorized (discard traffic).

    NOTE If the port 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.

- **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.
- **Termination Cause**—Displays the reason for which the port authentication was terminated, if applicable.

STEP 4 Click **Apply**. The port settings are defined, and the switch 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. (Port Security cannot be enabled on a port in single-host mode.)
- *Multiple Host (802.1X)*—Multiple hosts can be attached to a single 802.1X-enabled port. Only the first host must be authorized, and then the port is wide-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 number of specific authorized hosts to access the port. Each host is treated as if it were 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 *Host and Session Authentication Page* displays.

802.1X authentication parameters are described for all ports. All fields except the following are described in the *Edit Host and Session Authentication Page*.

- **Status**—Displays the host status. An asterisk indicates that the port is either not linked or is down. The options are:
  - *Unauthorized*—Either the port control is *Force Unauthorized* and the port link is down, or the port control is *Auto* but a client has not been authenticated via the port.
  - *Force-Authorized*—Clients have full port access.
  - *Single-host Lock*—Port control is *Auto* and only a single client has been authenticated by using the port.
  - *No Single Host*—Port control is *Auto* and Multiple Hosts mode is enabled. At least one client has been authenticated.
  - *Not in Auto Mode*—Auto port control is not enabled.
- **Number of Violations**—Displays the number of packets that arrive on the interface in single-host mode, from a host whose MAC address is not the supplicant MAC address.

STEP 2 Select a port, and click **Edit.** The *Edit Host and Session Authentication Page* displays.

STEP 3 Enter the parameters.

- **Port**—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*.

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:
  - *Discard*—Discards the packets.
  - *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.

  NOTE Traps on the 200 Series are syslog related and not SNMP.

- **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 switch is updated.

Viewing Authenticated Hosts

The *Authenticated Hosts Page* displays details about those users that have been authenticated. These details include such details as the username used to authenticate the user, the station MAC address, and the length of time that the user has been logged on.

To view details about authenticated users:

STEP 1 Click **Security** > **802.1X** > **Authenticated Hosts**. The *Authenticated Hosts Page* displays.

This page displays the following fields:

- **User Name**—Supplicant names that were authenticated on each port.
- **Port**—Number of 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. The options are:
  - *None*—No authentication is applied; it is automatically authorized.
  - *RADIUS*—Supplicant was authenticated by a RADIUS server.
- **MAC Address**—Displays the supplicant MAC address.

17

Configuring Quality of Service

The Quality of Service feature is applied throughout the network to ensure that network traffic is prioritized according to required criteria and the desired traffic receives preferential treatment.

This chapter contains the following topics:

QoS Features and Components

The QoS feature is used to optimize network performance.

QoS provides the following:

- Classification of incoming traffic to traffic classes, based on attributes, including:
  - Device Configuration
  - Ingress interface
  - Packet content
  - Combination of these attributes

QoS includes the following:

- **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.
- **Other Traffic Class-Handling Attribute**—Applies QoS mechanisms to various classes, including bandwidth management.

QoS Workflow

To configure general QoS parameters, perform the following:

STEP 1 Enable QoS by using the *QoS Properties Page* to select the trust mode.

STEP 2 Assign each interface a default CoS or DSCP priority by using the *QoS Properties Page*.

STEP 3 Assign the schedule method (Strict Priority or WRR) and bandwidth allocation for WRR to the egress queues by using the *Queue Page*.

STEP 4 Designate an egress queue to each IP DSCP/TC value with the *DSCP to Queue* Page. If the switch is in DSCP trusted mode, incoming packets are put into the egress queues based on the their DSCP/TC value.

STEP 5 Designate an egress queue to each CoS/802.1p priority. If the 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. This is done by using the *CoS/802.1p to Queue Page*.

STEP 6 Enter bandwidth and rate limits in the following pages:

a. Set egress shaping per queue by using the *Egress Shaping Per Queue Page.*

b. Set ingress rate limit and egress shaping rate per port by using the *Bandwidth Page.*

Configuring QoS

Displaying QoS Properties

The *QoS Properties Page* contains fields for enabling QoS and selecting the trust mode to be used. In addition, the default CoS priority or DSCP value for each interface can be defined.

To enable QoS:

STEP 1 Click **Quality of Service** > **General** > **QoS Properties**. The *QoS Properties Page* opens.

STEP 2 Enable QoS on the switch.

STEP 3 Select a trust mode (CoS/802.1p or DSCP) and click **Apply**.

STEP 4 If you selected DSCP, proceed to **STEP 6**; if you selected CoS, proceed to the next step.

STEP 5 Select **Port/LAG** to display/modify all ports/LAGs and their CoS information.

The following fields are displayed for all ports/LAGs:

- **Interface**—Type of interface.
- **Default CoS**—Default VPT value for incoming packets that do not have a VLAN Tag. The default CoS is 0. The default is only relevant for untagged frames if *Trust CoS* is selected.

Select **Restore Defaults** to restore the factory CoS default setting for this interface.

STEP 6 Click **DSCP Override Table** to enter the DSCP values. The *DSCP Override Table* opens.

STEP 7 DSCP In displays the DSCP value of the incoming packet that needs to be remarked to an alternative value. Select the new DSCP value to override the incoming value.

Select Restore Defaults to restore the factory DSCP values.

STEP 8 Click **Apply**. The switch is updated.

Modifying Interface Default CoS Value

STEP 1 Click **Quality of Service** > **General** > **QoS Properties**. The *QoS Properties Page* opens.

STEP 2 Select an interface, and click **Edit**. The *Edit Interface CoS Configuration Page* opens.

STEP 3 Enter the parameters.

- **Interface**—Select the interface.
- **Default CoS**—Select the default CoS (Class-of-Service) value to be assigned for incoming packets (that do not have a VLAN tag). The range is 0-7.

STEP 4 Click **Apply**. The interface default CoS value is set, and the switch is updated.

Defining QoS Interface Settings

The *Interface Settings Page* enables configuring QoS on each port of the switch, as follows:

QoS State Disabled on an Interface—All inbound traffic on the port is mapped to the best effort queue and no classification/prioritization takes place.

QoS State Enabled on an Interface—Port prioritized traffic on ingress is based on the system-wide configured trusted mode, which is either CoS/802.1p or DSCP trusted mode.

To enter QoS settings per interface:

STEP 1 Click **Quality of Service** > **Interface Settings**. The *Interface Settings Page* opens.

STEP 2 Select **Port** or **LAG** to display the list of ports or LAGs.

The list of ports/LAGs is displayed. **QoS State** displays whether QoS is enabled on the interface.

STEP 3 Select an interface, and click **Edit**. The *Edit QoS Interface Settings* opens.

STEP 4 Select either the **Port** or **LAG** to be modified.

STEP 5 Click to enable or disable **QoS State** for this interface.

STEP 6 Click **Apply**. The switch is updated.

Configuring QoS Queues

The switch supports four queues for each interface. Queue number four is the highest priority queue. Queue number one is the lowest priority queue.

There are two ways of determining how traffic in queues is handled, Strict Priority and Weighted Round Robin (WRR).

Strict Priority—Egress traffic from the highest-priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, thus providing the highest level of priority of traffic to the highest numbered queue.

Weighted Round Robin (WRR)—In WRR mode the number of packets sent from the queue is proportional to the weight of the queue (the higher the weight the more frames are sent). For example, if all four queues are WRR and the default weights are used, queue 1 receives 1/15 of the bandwidth (assuming all queues are saturated and there is congestion), queue 2 receives 2/15, queue 3 receives 4/15 and queue 4 receives 8 /15 of the bandwidth. The type of WRR algorithm used in the device is not the standard Deficit WRR (DWRR), but rather Shaped Deficit WRR (SDWRR).

The queuing modes can be selected in the *Queue Page.* When the queuing mode is by strict priority, the priority sets the order in which queues are serviced, starting with queue_4 (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 strict priority queues is always sent before traffic from the WRR queues. Only after the strict priority queues have been emptied is traffic from the WRR queues forwarded. (The relative portion from each WRR queue depends on its weight).

To select the priority method and enter WRR data.

STEP 1 Click **Quality of Service** > **General** > **Queue**. The *Queue Page* opens.

STEP 2 Enter the parameters.

- **Queue**—Displays the queue number.
- **Scheduling Method:** Select one of the following options:
  - **Strict Priority**—Traffic scheduling for the selected queue and all higher queues is based strictly on the queue priority.
  - **WRR**—Traffic scheduling for the selected queue is based on WRR. The period time is divided between the WRR queues that are not empty, meaning they have descriptors to egress. This 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 configured, and the switch is updated.

Mapping CoS/802.1p to a Queue

The *CoS/802.1p to Queue Page* maps 802.1p priorities to egress queues. The CoS/802.1p to Queue Table determines the egress queues of the incoming packets based on the 802.1p priority in their VLAN Tags. For incoming untagged packets, the 802.1p priority will be the default CoS/802.1p priority assigned to the ingress ports.

Default Mapping Queues

802.1p Values (0-7, 7 being the highest)	Queue (4 queues 1-4, 4 being the highest priority)	Notes
0	1	Background
1	1	Best Effort
2	2	Excellent Effort
3	3	Critical Application LVS phone SIP
4	3	Video
5	4	Voice Cisco IP phone default
6	4	Interwork Control LVS phone RTP
7	4	Network Control

By changing the CoS/802.1p to Queue mapping and the Queue schedule method and bandwidth allocation, it is possible to achieve the desired quality of services in a network.

CoS/802.1p to Queue mapping is applicable only if CoS/802.1p is the trusted mode and the packets belong to flows that are CoS trusted.

To map CoS values to egress queues:

STEP 1 Click **Quality of Service** > **General** > **CoS/802.1p to Queue**. The *CoS/802.1p to Queue Page* opens.

STEP 2 Enter the parameters.

- **802.1p**—Displays the 802.1p priority tag values to be assigned to an egress queue, where 0 is the lowest and 7 is the highest priority.
- **Output Queue**—Select the egress queue to which the 802.1p priority is mapped. Four egress queues are supported, where Queue 4 is the highest priority egress queue and Queue 1 is the lowest priority.
- **Restore Defaults**—Click to restore all queues to the factory default CoS/802.1pto Queue mapping.

STEP 3 For each 802.1p priority select the Output Queue to which it is mapped.

STEP 4 Click **Apply**. 801.1p priority values to queues are mapped, and the switch is updated.

Mapping DSCP to Queue

The DSCP (IP *Differentiated Services Code Point*) to Queue Page maps 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 VPT (VLAN Priority Tag) of the packet is unchanged.

By simply changing the DSCP to Queue mapping and the Queue schedule method and bandwidth allocation, it is possible to achieve the desired quality of services in a network.

DSCP to Queue mapping is applicable to IP packets if DSCP is the trusted mode.

Non-IP packets are always classified to the best-effort queue.

To map DSCP to queues:

STEP 1 Click **Quality of Service** > **General** > **DSCP to Queue**. The *DSCP to Queue Page* opens.

The *DSCP to Queue Page* contains **Ingress DSCP**. It displays the DSCP value in the incoming packet and its associated class.

STEP 2 Select the **Output Queue** (traffic forwarding queue) to which the DSCP value is mapped.

STEP 3 Click **Apply**. The switch is updated.

Configuring Bandwidth

The *Bandwidth Page* enables network managers to define two sets of values that determine how much traffic the system 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.

The following values are entered for egress shaping:

- Committed Information Rate (CIR) sets the average maximum amount of data allowed to be sent on the egress interface, measured in bits per second
- Committed Burst Size (CBS) is the burst of data that is allowed to be sent, even though it is above the CIR. This is defined in number of bytes of data.

To enter bandwidth limitation:

STEP 1 Click **Quality of Service** > **General** > **Bandwidth**. The *Bandwidth Page* opens.

The *Bandwidth Page* displays bandwidth information for each interface.

The % column is the ingress rate limit for the port divided by the total port bandwidth.

STEP 2 Select an interface, and click **Edit**. The *Edit Bandwidth Page* opens.

STEP 3 Select the **Port/LAG** interface.

STEP 4 Enter the fields for the selected interface:

- **Ingress Rate Limit**—Select to enable the ingress rate limit, which is defined in the field below.
- **Ingress Rate Limit**—Enter the maximum amount of bandwidth allowed on the interface.

  NOTE The two **Ingress Rate Limit** fields do not appear when the interface type is LAG.
- **Egress Shaping Rate**—Select to enable egress shaping on the interface.
- **Committed Information Rate (CIR)**—Enter the maximum bandwidth for the egress interface.
- **Committed Burst Size (CBS)**—Enter the maximum burst size of data for the egress interface in bytes of data. This amount can be sent even if it temporarily increases the bandwidth beyond the allowed limit.

STEP 5 Click **Apply**. The bandwidth settings are modified, and the switch is updated.

Configuring Egress Shaping per Queue

In addition to limiting transmission rate per port, which is done in 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.

To define egress shaping per queue:

STEP 1 Click **Quality of Service** > **General** > **Egress Shaping per Queue**. The *Egress Shaping Per Queue Page* opens.

The *Egress Shaping Per Queue Page* displays the rate limit and burst size for each queue.

STEP 2 Select an interface type (Port or LAG), and click **Go**. The list of ports/LAGs is displayed.

STEP 3 Select a port/LAG, and click **Edit**. The *Edit Egress Shaping Per Queue Page* opens.

This page enables shaping the egress for up to four queues on each interface.

STEP 4 Select the **Interface**.

STEP 5 For each queue that is required, enter the following fields:

- **Enable Shaping**—Select to enable egress shaping on this queue.
- **Committed Information Rate (CIR)**—Enter the maximum rate (CIR) in Kbits per second (Kbps). CIR is the average maximum amount of data that can be sent.
- **Committed Burst Size (CBS)**—Enter the maximum burst size (CBS) in bytes. CBS is the maximum burst of data allowed to be sent even if a burst exceeds CIR.

STEP 6 Click **Apply**. The bandwidth settings are modified, and the switch is updated.

Managing QoS Statistics

The *Queues Statistics Page* displays queue statistics, including statistics of forwarded and dropped packets, based on interface, queue, and drop precedence.

To view Queues Statistics:

STEP 1 Click **Quality of Service** > **QoS Statistics** > **Queues Statistics**. The *Queues Statistics Page* opens.

This page displays the following fields:

- **Refresh Rate**—Select how often the statistics will be refreshed or *No Refresh* if they are not to be refreshed at all.

Queues Statistics Table

- **Counter Set**—The options are:
  - *Set 1*—Displays the statistics for Set 1 that contains all interfaces and queues with a high DP (Drop Precedence).

  - *Set 2*—Displays the statistics for Set 2 that contains all interfaces and queues with a low DP.

- **Interface**—Queue statistics are displayed for this interface.
- **Queue**—Packets were forwarded or tail dropped from this queue.
- **Drop Precedence**—Lowest drop precedence has the lowest probability of being dropped.
- **Total packets**—Number of packets forwarded or tail dropped.
- **Tail Drop packets**—Percentage of packets that were tail dropped.

STEP 2 Click **Add.** The *Add Queues Statistics Page* opens.

STEP 3 Enter the parameters.

- **Counter Set**—Select the counter set:
  - *Set 1*—Displays the statistics for Set 1 that contains all interfaces and queues with a high DP (Drop Precedence).
  - *Set 2*—Displays the statistics for Set 2 that contains all interfaces and queues with a low DP.
- **Interface**—Select the ports for which statistics are displayed. The options are:
  - *Port*—Selects the port on the selected unit number for which statistics are displayed.
  - *All Ports*—Specifies that statistics are displayed for all ports.
- **Queue**—Select the queue for which statistics are displayed.
- **Drop Precedence**—Enter drop precedence that indicates the probability of being dropped.

STEP 4 Click **Apply.** The Queue Statistics counter is added, and the switch is updated.

OL-22849-01