ADMINISTRATION GUIDE

Cisco Small Business

SG200 Series 8-port Smart Switches

Contents

1

Getting Started

This chapter provides an introduction to the web-based switch configuration utility and includes the following topics:

- **Starting the Web-Based Switch Configuration Utility**
- **Quick Start Device Configuration**
- **Window Navigation**

Starting the Web-Based Switch Configuration Utility

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

Browsers have the following restrictions:

- If you are using Internet Explorer 8, open a browser window and configure the following settings:

  Click **Tools** > **Internet Options** and then select the **Security** tab. Select **Local Intranet** and click **Sites**. Click **Advanced** and then click **Add**. Add the intranet address of the switch (http://*<ip-address>*) to the local intranet zone. The IP address can also be specified as the subnet IP address, so that all addresses in the subnet are added to the local intranet zone.

- If you are using Internet Explorer 6, you cannot directly use an IPv6 address to access the switch. You can, however, use the Domain Name System (DNS) 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.

- Screen resolutions at 800x600 or lower in Internet Explorer browsers and Firefox 3.6 are not supported by the web-based switch configuration utility.

Launching the Utility

To open the web-based switch configuration utility:

STEP 1 Open a web browser.

STEP 2 Enter the IP address of the switch that you are configuring in the address bar on the browser, and then press **Enter**. (The factory default IP address is **192.168.1.254**.) The *Log In* page opens.

Logging In

To log in to the web-based switch configuration utility:

STEP 1 Enter the *username* and *password*. The factory default user name is **cisco** and the default password is **cisco**.

Note: When the switch boots with the factory default configuration, the web-based switch configuration utility appears in the default language. After you log in, you can download additional languages by using the *Upgrade/Backup Firmware/Language* page.

STEP 2 If this is the first time that you logged on with the default user name (**cisco**) and the default password (**cisco**) or your password has expired, the *Change Admin Password* page opens. Enter the new password, confirm it, click **Apply**, and then click **Close**. (The characters ', ", %, and ? are not supported.) The new password is saved.

NOTE Password complexity is enabled by default and the new password must comply to the default password complexity rule defined by the password strength. (See **Adding a User** for more information.) The password strength check can be temporarily disabled by selecting the Disable Password Strength Enforcement option.

STEP 3 Click **Login**.

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

If you entered an incorrect user name or password, an error message is displayed and the *Log In* page remains displayed on the screen.

NOTE When logging in by using HTTP or HTML, if you are provided an option to choose from more than one network port, select the lowest number port.

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

Logging Out

By default, the application automatically logs you out after 10 minutes of inactivity. See **Configuring the Idle Session Timeouts** for instructions on changing the default timeout period.

To log out at any time, click **Logout** in the top right corner of any page.

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

A red **X** icon displayed to the left of the Save button indicates that Running Configuration changes have been made that have not yet been saved to the Startup Configuration file type.

When you click **Save**, the **Download/Backup Configuration/Log** page displays (see **Downloading and Backing Up the Configuration and Log Files**). Save the Running Configuration by copying it to the Startup Configuration file type. After this save, the red **X** icon and the Save button no longer display.

Quick Start Device Configuration

To simplify device 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*
	Create VLAN	*Create VLAN*
	Configure Port Settings	*Port Settings*
Device Status	System Summary	*System Summary*
	Port Statistics	*Interface*
	RMON Statistics	*RMON Statistics*
	View Log	*RAM Memory*
Quick Access	Change Device Password	*User Accounts*
	Upgrade Device Software	*Upgrade/Backup Firmware/ Language*
	Backup Device Configuration	*Download/Backup Configuration/ Log*
	Configure QoS	*QoS Properties*
	Configure Port Mirroring	*Port Mirroring*

Window Navigation

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 buttons:

Buttons

Name	Description
	The Syslog Alert Status button (red circle with an **X**) is displayed when a new Syslog message, above the critical severity level, is logged. Click to open the Status and **Statistics** > **View Log** > *RAM Memory Log* page. After you access this page, the Syslog Alert Status button is no longer displayed.
	A red **X** icon, displayed to the left of the Save button, indicates that configuration changes have been made and have not yet been saved to the Startup Configuration file. When you click this button, the *Download/Backup Configuration/Log* page displays. Save the Running Configuration by copying it to the Startup Configuration file type. After you click **Apply** to save this file, the red X icon and the Save button 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.
User	The name of the user logged on to the switch. The default user name is **cisco**.
Language Menu	Select a language or load a new language file into the device. If the language required is displayed in the menu, select it. If not, select **Download Language**. For more information about adding a new language, refer to the *Upgrade/Backup Firmware/Language* page.

Buttons (Continued)

Name	Description
Log Out	Click to log out of the web-based switch configuration utility.
About	Click to display the switch type and switch version number.
Help	Click to display the online help.

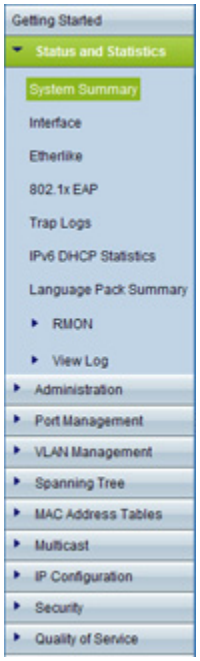
Other Resources

You can use the following links on the Getting Started page for additional information and assistance with using your switch:

- **Support**—Displays the support web page for Cisco Small Business Managed Switches.
- **Forums**—Displays the web page for the Cisco Small Business Support Community.

Navigation Window

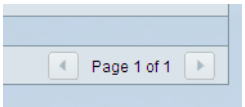
A navigation window is located on the left side of each page. Click a top-level category to display links to related pages. Links that are preceded by an arrow are subcategories that expand to display the related page links.



Management Buttons

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

Management Buttons

Name	Description
	Depending on the number of pages and the currently displayed page, use these features to navigate through the pages of the table. Click **I<** to go to the first page, click **<** to go to the previous page, click **>** to go to the next page, and click **>I** to go to the last page. Use the **Page** *<number>* **of** *<number>* drop-down list to choose a particular page.

Management Buttons (Continued)

Name	Description
	Select the number of table entries to display on each page.
	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**. Click **Close** to return to the main page. **Note:** Your changes are applied to the running configuration only. If the switch is rebooted, the running configuration is lost. To save your changes to the startup configuration, click **Save**. For more information, see **Copying and Saving Configuration Files**.
Apply	Click to apply the changes that you entered on the selected page. **Note:** Your changes are applied to the running configuration only. If the switch is rebooted, the running configuration is lost. To save your changes to the startup configuration, click **Save**. For more information, see **Copying and Saving Configuration Files**.
Cancel	Click to “undo” the changes that you made on the page and to reset the values to the previously applied entries.
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	Click to clear the log files.
Clear Table	Click to clear the table entries.
Close	Click to return to the main page. If there are changes that were not applied to the Running Configuration, a message is displayed.

Management Buttons (Continued)

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: ▪ Select the entry to be copied. Click **Copy Settings**. ▪ Enter the destination entry numbers. ▪ Click **Apply** to save the changes to the Running Configuration. ▪ Click **Close** to return to the main page.
Delete	Select the entry in the table to be deleted and click **Delete**. The entry is deleted.
Details	Click to display details associated with the entry selected on the main page.
Edit	Select an entry and click **Edit** to open it for editing. The *Edit* page opens, and the entry can be modified. ▪ Click **Apply** to save the changes to the Running Configuration. (Note that there is no message to confirm that the parameters have been saved to the Running Configuration. This is normal behavior.) ▪ Click **Close** to return to the main page.
Test	Click **Test** to perform related tests.
Clear Filter	Click **Clear Filter** to redisplay data on a page with the default criteria.
Go	Click **Go** to filter the data displaying on a page using the selected criteria.

Management Buttons (Continued)

Name	Description
Sort buttons	If the *This table is sortable* message appears below a table, each column heading is a sort button. Click a column heading to sort the records in ascending order, based on the contents of the selected column. After the sort is applied, an arrow appears in the column heading. You can click this arrow to reverse the sort order.

2

Viewing Statistics

This chapter describes how to display switch statistics.

It contains the following topics.

System Summary

The *System Summary* page displays basic information such as the hardware model description, software version, language packs, and system up time.

Displaying the System Summary

To view system information, click **Status and Statistics** > **System Summary** in the navigation window. Or, click **System Summary** under **Device Status** on the *Getting Started* page.

The System Summary page displays the following information:

- **System Description**—A description of the system.
- **System Location**—Physical location of the switch. Click **Edit** to display the *System Settings* page and enter this value. (The characters ', ", %, and ? are not supported.)

- **System Contact**—Name of a contact person. Click **Edit** to display the *System Settings* page and enter this value. (The characters ', ", %, and ? are not supported.)
- **Hostname**—Name of the switch. Click **Edit** to display the *System Settings* page and 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 base object ID for the system's management information base (MIB).
- **System Uptime**—Time that has elapsed since the last reboot.
- **Current Time**—Current system time.
- **Base MAC Address**—Switch MAC address.

Hardware and Firmware Version Information

The following hardware and software information displays for the switch:

- **Serial Number**—Serial number of the switch.
- **PID VID**—Part number and version ID.
- **Boot Version**—Version of the boot code.
- **Maximum Available Power (W)**—(PoE switches only) Maximum available power that can be delivered by the PoE ports.
- **Threshold Power**—(PoE switches only) The amount of power that must be available for delivery in order for the port to be powered up.
- **Consumed Power**—(PoE switches only) Power currently being delivered to the PoE devices connected to the switch.
- **Firmware Version**—Firmware version number of the active image.
- **Firmware MD5 Checksum**—MD5 checksum of the active image.
- **Boot MD5 Checksum**—MD5 checksum of the boot code.

You can view settings for each switch port. To display the *Port Settings* page, click the port.

Language Pack Table

This table displays information about the languages available on the switch. A language can be selected by the administrator when logging into the configuration utility.

English is the default language and it is built into the software. You can use the *Upgrade/Backup Firmware/Language* page to download additional language packs. Language files are available from the Cisco firmware download page.

The Language Pack Table displays the following information for each available language:

- **Language**—Language name.
- **Locale**—Internet Engineering Task Force (IETF) locale code that identifies the language and the country or region.
- **Version**—Language file version.
- **MD5 Checksum**—128-bit hash code used to check file integrity.
- **File Size**—The file size in KB.
- **File Type**—Indicates one of the following values:
  - **Built-In**—Default language provided within the software and therefore cannot be downloaded as a separate file.
  - **External**—A language file that has been downloaded to the switch and can be selected at login.
- **Default**—Displays **Yes** to indicate that the web-based switch configuration utility login page will display in this language whenever the switch is rebooted.
- **Status**—Displays **Active** or **Inactive**. At log-in, the user can choose a language. The selected language is the Active language.
- **Number of Users**—The number of management users currently logged in and using this language.

TCP and UDP Services

This table lists the information for each service that uses TCP or UDP:

- **Service Name**—The commonly–used name of the service, if available, such as HTTP.
- **Type**—The transport protocol used for this service (TCP or UDP).

- **Port**—The Internet Assigned Numbers Authority (IANA) port number for the service.
- **IP Address**—The IP address, if any, of a remote device that is connected to this service on the switch.
- **Remote Port**—The IANA port number of any remote device communicating with this service.
- **State**—The state of the service. For UDP, only connections in the Active state display in the table. In the Active state, a connection is established between the switch and a client or server. The TCP states are:
  - **Listen**—The service is listening for connection requests.
  - **Active**—A connection session is established and packets are being transmitted and received.
  - **Established**—A connection session is established between the switch and a server or client, depending on each device's role with respect to this protocol.

Configuring System Settings

To configure the system settings:

STEP 1 Click **Status and Statistics** > **System Summary**. The *System Summary* page opens.

STEP 2 Click **Edit** to modify the following settings:

- **System Location**—Enter the location where the switch is physically located.
- **System Contact**—Enter the name of a contact person.
- **Hostname**—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, RFC1034, and RFC1035). The default hostname is the word **`switch`** followed by the last three octets of the base MAC address. For example, a switch with a MAC address of 010203040506 has the default hostname **`switch040506`**.

STEP 3 Click **Apply**. Your changes are saved to the Running Configuration.

Interface Statistics

Use the *Interface* page to display statistics for received and transmitted packets. To display this page, click **Status and Statistics** > **Interface** in the navigation window, or click **Port Statistics** under **Device Status** on the *Getting Started* page.

Select the interface (Port or LAG) for which you want to display statistics, then select a refresh rate for the statistics. The following information displays for the selected interface:

- **Total Bytes (Octets)**—Total number of octets transmitted or received on the selected interface since the switch was last refreshed.
- **Unicast Packets**—Total number of unicast packets transmitted or received on the selected interface since the switch was last refreshed.
- **Multicast Packets**—Total number of multicast packets transmitted or received on the selected interface since the switch was last refreshed.
- **Broadcast Packets**—Total number of broadcast packets transmitted or received on the selected interface since the switch was last refreshed.
- **Packets with Errors**—Total number of packets with errors received on the selected interface since the switch was last refreshed.
- **STP BPDUs**—Total number of Spanning Tree Protocol (STP) Bridge Protocol Data Units (BPDUs) transmitted or received on the selected interface since the switch was last refreshed.
- **RSTP BPDUs**—Total number of Rapid Spanning Tree Protocol BPDUs transmitted or received on the selected interface since the switch was last refreshed.

To clear statistics counters:

Click **Clear Interface Counters** to reset all counters to 0 for the selected interface.

Click **Clear All Interface Counters** to reset all counters to 0 for all interfaces.

Etherlike Statistics

The system collects and reports statistics on ports and LAGs in accordance with RFC2665.

To display this page, click **Status and Statistics** > **Etherlike** in the navigation window.

Select the interface (Port or LAG) for which you want to display statistics, then select a refresh rate for the statistics. These statistics are cumulative since the last time the page was refreshed. The following information displays for the selected interface:

- **Frame Check Sequence (FCS) Errors**—FCS errors received.
- **Single Collision Frames**—Signal collision frame errors received.
- **Late Collisions**—Late collision frames received.
- **Excessive Collisions**—Excessive collision frames received.
- **Multiple Collisions**—Multiple collision frames received.
- **Oversize Packets**—Packets received that were longer than 1518 octets (excluding framing bits and including FCS octets) and were otherwise well-formed.
- **Internal MAC Receive Errors**—Internal MAC errors received on the LAG or interface.
- **Alignment Errors**—Packets received with alignment errors
- **Pause Frames Received**—Pause frames received on the LAG or interface.
- **Pause Frames Transmitted**—Pause frames transmitted from the LAG or interface.

To clear statistics counters:

Click **Clear Interface Counters** to reset all counters to 0 for the selected interface.

Click **Clear All Interface Counters** to reset all counters to 0 for all interfaces.

802.1X EAP Statistics

The switch ports can be configured to use the IEEE 802.1X Extensible Authentication Protocol (EAP) to control network access (see **802.1X**). You can use the *802.1X EAP* page to display information about EAP packets received on a port.

To display the 802.1X EAP page, click **Status and Statistics** > **802.1X EAP** in the navigation window.

STEP 1 Select the **Port** for which you want to display statistics.

STEP 2 Select a **Refresh Rate** for the statistics. These statistics are cumulative since the last time the page was refreshed.

The following information displays for the selected interface:

- **EAPOL Frames Received**—Valid Extensible Authentication Protocol over LAN (EAPOL) frames received on the port.
- **EAPOL Frames Transmitted**—EAPOL frames transmitted through the port.
- **EAPOL Start Frames Received**—EAPOL Start frames received on the port.
- **EAPOL Logoff Frames Received**—EAPOL Logoff frames received on 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.

To clear statistics counters:

Click **Clear Interface Counters** to reset all counters to 0 for the selected interface.

Click **Clear All Interface Counters** to reset all counters to 0 for all interfaces.

IPv6 DHCP Statistics

The switch can be configured to allow management over an IPv6 interface, and to receive its management IPv6 address through the Dynamic Host Configuration Protocol (DHCPv6). See **Management Interface** for information on configuring IPv6 and DHCP on the management interface. You can use the *IPv6 DHCP Statistics* page to display information on transmitted and received DHCPv6 packets.

To display this page, click **Status and Statistics** > **IPv6 DHCP Statistics** in the navigation window.

Select a refresh rate for the page. The page displays the following statistics, which are cumulative since the last time the page refreshed.

- DHCPv6 Advertisement Packets Received
- DHCPv6 Reply Packets Received
- Received DHCPv6 Advertisement Packets Discarded
- Received DHCPv6 Reply Packets Discarded
- DHCPv6 Malformed Packets Received
- Total DHCPv6 Packets Received
- DHCPv6 Solicit Packets Transmitted
- DHCPv6 Request Packets Transmitted
- DHCPv6 Renew Packets Transmitted
- DHCPv6 Rebind Packets Transmitted
- DHCPv6 Release Packets Transmitted
- Total DHCPv6 Packets Transmitted

Click **Clear Counters** to reset all counters to 0.

RADIUS Statistics

The switch can be configured to communicate with a RADIUS server for user authentication. To display the *RADIUS Statistics* page, click **Status and Statistics** > **RADIUS Statistics** in the navigation window.

Select a RADIUS server from the list and select a refresh rate for the page. The page displays the following statistics, which are cumulative since the last time the page refreshed.

- **Access Requests**—The number of Authentication-Request packets transmitted to the RADIUS server.
- **Access Retransmissions**—Number of Authentication-Request packets retransmitted to the RADIUS server.
- **Access Accepts**—Number of Authentication-Request packets accepted by the RADIUS server.
- **Access Rejects**—Number of Authentication-Request packets rejected by the RADIUS server.
- **Access Challenges**—Number of Access-Challenge packets sent by the RADIUS server to the switch.
- **Malformed Access Responses**—Number of reply packets from the RADIUS server that were malformed.
- **Bad Authenticators**—Number of Authentication-Request packets that contained invalid Message Authenticator attributes.
- **Pending Requests**—Number of Authentication-Request packets that were sent to the server and have not been replied to.
- **Timeouts**—Number of Authentication-Request packets that were timed out due to no response from the server.
- **Unknown Types**—Number of RADIUS packets of unknown type that were received by the switch.
- **Packets Dropped**—Number of RADIUS packets dropped by the switch.

Click **Clear All Statistics** to reset all counters to 0.

RMON

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

RMON decreases the traffic between the manager and the switch because the SNMP manager does not have to frequently poll the switch for information, and enables the manager to get timely status reports because the switch reports events as they occur. Use the *RMON Statistics* page to display details about switch use, such as packet processing statistics and errors that have occurred on the switch.

The *RMON Statistics* page displays detailed information regarding packet sizes and information regarding physical layer errors. The information shown is according to the RMON standard.

To view statistics:

STEP 1 Click **Status and Statistics** > **RMON** > **Statistics** in the navigation window.

STEP 2 Select the port or LAG for which you want to display statistics.

STEP 3 Select a refresh rate for the page.

The following information displays for the selected interface:

- **Bytes Received**—Octets received on the interface since the switch was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Drop Events**—Number of times that packets have been dropped on the interface since the switch was last refreshed.
- **Packets Received**—Packets received on the interface, including bad packets, multicast and broadcast packets, since the switch was last refreshed.
- **Broadcast Packets Received**—Good broadcast packets received on the interface since the switch was last refreshed. This number does not include multicast packets.

- **Multicast Packets Received**—Good multicast packets received on the interface since the switch was last refreshed.
- **CRC & Align Errors**—CRC and Align errors that have occurred on the interface since the switch was last refreshed.
- **Undersize Packets**—Undersized packets (less than 64 octets) received on the interface since the switch was last refreshed.
- **Oversize Packets**—Oversized packets (over 1518 octets) received on the interface since the switch was last refreshed.
- **Fragments**—Fragments (packets with less than 64 octets, excluding framing bits, but including frame check sequence octets) received on the interface since the switch was last refreshed.
- **Jabbers**—Packets received that were more than 1518 octets long and had an FCS error during the sampling session.
- **Collisions**—Collisions received on the interface since the switch was last refreshed.
- **Frames of 64 Bytes**—64-byte frames received on the interface since the switch was last refreshed.
- **Frames of 65 to 127 Bytes**—65-byte to 127-byte frames received on the interface since the switch was last refreshed.
- **Frames of 128 to 255 Bytes**—128-byte to 255-byte frames received on the interface since the switch was last refreshed.
- **Frames of 256 to 511 Bytes**—256-byte to 511-byte frames received on the interface since the switch was last refreshed.
- **Frames of 512 to 1023 Bytes**—512-byte to 1023-byte frames received on the interface since the switch was last refreshed.
- **Frames of 1024 to 1518 Bytes**—1024-byte to 1518-byte frames received on the interface since the switch was last refreshed.

Logs

The switch generates messages to identify the state of the system and to assist in diagnosing issues that arise during switch operation. Messages might be generated in response to events, faults, or errors occurring on the platform and to changes in configuration.

Logs of these messages are stored in RAM and flash memory. Entries in the flash log—unlike those in RAM—are stored across reboots.

To access the log menu items, click **Status and Statistics** > **View Log** in the navigation window. The log menu includes the following pages:

- **RAM Memory Log**
- **Flash Memory Log**

RAM Memory Log

Use the *RAM Memory* page to view information about specific RAM (cache) log entries, including the time the log was entered, the log severity, and a description of the log.

To display this page, click **Status and Statistics** > **View Log** > **RAM Memory** in the navigation window.

NOTE This page might take up to 45 seconds to display when the table contains the maximum number of entries.

The RAM Memory Log Table contains the following fields:

- **Log Index**—Numeric ID for the log entry.
- **Log Time**—Time at which the log was entered in the Log RAM Table.
- **Severity**—The log severity can be one of the following:
  - **Emergency (0)**—System is unusable.
  - **Alert (1)**—Action must be taken immediately.
  - **Critical (2)**—Critical conditions.
  - **Error (3)**—Error conditions.
  - **Warning (4)**—Warning conditions.
  - **Notice (5)**—Normal but significant conditions.

- **Informational (6)**—Informational messages.
- **Debug (7)**—Provides detailed information about an event.

You can use the *Log Settings* page to select the severity levels that are recorded in the log.

- **Component** - The software component or service that produced the log entry.
- **Description**—The log description.

You can click **Clear Logs** to remove all log entries from RAM.

Flash Memory Log

The Flash Memory Log Files are persistent across reboots and contain information that includes the time the log was entered, the log severity, and a description of the event. Several log *types* are supported, and the system stores up to three versions of each type.

The first few log entries that might be generated during the initial powering on of the switch and booting from the factory default configuration might be important to a troubleshooter. Therefore when the switch is first booted from the factory default configuration, it places the first 32 messages into the Start-up log and the balance of the messages are logged into the Operational log.

If the logs are cleared, the Start-up log is retained unless the switch is booted from the factory default configuration. Only when the switch is booted from the factory default configuration is the Start-up log cleared and repopulated.

To view a Flash log:

STEP 1 Click **Status and Statistics** > **View Log** > **Flash Memory** in the navigation window.

STEP 2 Select a log type from the list:

- **Default**—Entries from the startup and operational logs.
- **Startup**—The first 32 log entries created during system restarts.
- **Operational**—Log entries created during system operation.

STEP 3 Select a log version to display.

The Version 1 log is the current or most recently created log file, the Version 2 log is the next most recent, and the Version 3 log is the oldest file. When a new log file of the specified type is created, the Version 3 log is deleted and the Version 1 and Version 2 logs are renamed to Version 2 and Version 3, respectively.

When a different version and log is selected, the new log automatically displays in the Flash Memory Log Table. (When the table contains the maximum number of entries, this page might take up to 45 seconds to display.)

The Flash Memory Log Table contains the following fields:

- **Log Index**—Numeric ID for the log entry.
- **Log Time**—Time that the log was created in the Flash Memory Table.
- **Severity**—The log severity can be one of the following:
  - **Alert (1)**—Action must be taken immediately.
  - **Critical (2)**—Critical conditions.
  - **Error (3)**—Error conditions.
  - **Warning (4)**—Warning conditions.
  - **Notice (5)**—Normal but significant conditions.
  - **Informational (6)**—Informational messages.
  - **Debug (7)**—Provides detailed information about an event.

  You can use the *Log Settings* page to select the severity levels that are recorded in the log.
- **Component**—Software component that produced the log entry.
- **Description**—The log description.

Click **Clear Logs** to remove all log entries from flash memory.

Click **Backup Logs** to open the *Download/Backup Configuration/Log* page, where you can use TFTP or HTTP to back up the log files to a TFTP server or network location. For more information, see **Backing Up the Configuration File and Logs**.

3

Administration

This chapter describes how to configure global system settings and perform diagnostics.

It contains the following topics.

Configuring System Settings

The *System Settings* page enables you to configure information that identifies the switch within the network.

To configure system settings:

STEP 1 Click **Administration** > **System Settings** in the navigation window.

The System Description is hard-coded in the firmware.

STEP 2 Enter the parameters:

- **System Location**—Description of the physical location of the switch.
- **System Contact**—Contact person for the switch.
- **Hostname**—Administratively-assigned name for this managed node. By convention, this is the fully-qualified domain name of the node. The default hostname is **switch** concatenated with the last 6 hex digits of the MAC address of the switch. Hostname labels contain only letters, digits and hyphens. Hostname labels cannot begin or end with a hyphen. No other symbols, punctuation characters, or blank spaces are permitted.

  NOTE: You can check the Set Default field to return the hostname to the default.

STEP 3 Click **Apply**. The changes are saved to the Running Configuration.

Management Interface

Switch management interface enable access to the web-based switch configuration utility from a management station on the network. The switch supports configuration of a management VLAN that segregates the management traffic from other traffic on the switch.

The management interface can be configured with an IPv4 address or with an IPv6 address. The addresses can be configured statically or they can be obtained through DHCP/BOOTP servers.

See the following topics for more information on the configuration pages available in the **Administration** > **Management Interface** menu:

- **Configuring an IPv4 Management Interface**
- **Configuring an IPv6 Management Interface**
- **Viewing and Adding IPv6 Neighbors**

Configuring an IPv4 Management Interface

You can use the *IPv4 Interface* page to configure the management VLAN and IPv4 address.

To configure the IPv4 management interface:

STEP 1 Click **Administration** > **Management Interface** > **IPv4 Interface** in the navigation window.

STEP 2 Select a management VLAN from the list.

A port must be a member of the management VLAN to gain access to the web-based switch configuration utility. By default, VLAN 1 is configured as the management VLAN and all switch ports are configured as members of VLAN 1.

At least one port must be a member of the management VLAN. The Member Ports list displays all current members of the selected management VLAN.

Note that when you change the management VLAN, you must reassign any members of the previous management VLAN to the new VLAN to continue their management access.

STEP 3 Select one of the following options for the IP Address Type:

- **DHCP**—The management interface obtains its IPv4 address from a DHCP server. DHCP is enabled by default and the switch requests an IP address from a DHCP server. If it is unable to get the IP address from a server, the switch falls back to the factory default static IP address. The System LED flashes continuously and the switch keeps trying to get its IP address from a DHCP server. If you set a static IP address, the LED stops flashing. The factory default static IP address is 192.168.1.254/24, with a default gateway IP address of 192.168.1.1.
- **BOOTP**—The management interface obtains its IPv4 address from a BOOTP server.
- **Static**—The management interface IPv4 address assigned in the **IP Address** field.

  If the IP Address Type is set to Static, specify the following:

  - **IP Address**—Enter an IPv4 address.
  - **Mask**—Enter a 32-bit network mask (for example, 255.255.255.0). Or select **Prefix Length** and specify the number of bits (0–32) that make up the network prefix (for example, 24).
  - **Default Gateway**—Select **User Defined** and specify the default gateway IP address for management packets. Or select **None** to prevent management packets from being transmitted outside the subnet.
- **Operational Default Gateway**—The current default gateway in use.
- **Renew DHCP**—Select Renew DHCP and click Apply to send a request to the DHCP server for a new IP address and related parameters.

STEP 4 Click **Apply**. Your changes are saved to the Running Configuration.

CAUTION Changing the management IP address and IP Address Type terminates the current management session. Changing the Management VLAN and its port memberships might disrupt your communication with the switch and thus might terminate the current management session.

Configuring an IPv6 Management Interface

Use the *IPv6 Interface* page to enable access to the web-based switch configuration utility over IPv6. You can configure the switch to dynamically learn its IPv6 addresses and you can configure IPv6 addresses statically.

To enable IPv6 management access:

STEP 1 Click **Administration** > **Management Interface** > **IPv6 Interface** in the navigation window.

The Interface field shows the VLAN ID of the management VLAN.

STEP 2 Configure the following settings:

- **IPv6 Mode**—Select to enable IPv6 management access.
- **IPv6 Address Auto Configuration**—Select to enable the switch to auto-configure its link-local address(es) in EUI-64 format, using the MAC address of the port(s) for the link-local part of the address. The switch listens to router advertisements to detect and autoconfigure the global part of the address.
- **DHCPv6**—Select to enable the switch to obtain its IPv6 address(es) from a DHCPv6 server.
- **IPv6 Gateway**—Enter the link local address of the IPv6 router where the switch should send IPv6 packets destined for a device outside the subnet.

STEP 3 Click **Apply**. Your changes are saved to the Running Configuration. You can click **Cancel** to clear the changes.

Adding IPv6 Addresses

The IPv6 Address table lists static addresses currently configured on the switch. It contains the following fields:

- **IPv6 Address**—IPv6 address in IPv6 global address format.

  The table includes the default IPv6 address. The switch creates this address automatically by inserting standard byte values into its 48-bit MAC address to create a 64-bit IPv6 address in EUI-64 format, as described in RFC 3513.

- **DAD Status**—The Duplicate Address Detection status. When you configure an IPv6 address on the switch, before the switch actually assigns the address, it performs neighbor discovery to detect if that address is already in use on the network.
  - If the address is already in use, its DAD status is True, and the address is not usable for management access.
  - If the address is found to be unique, its DAD status is False, and the address can be used for management access.

You can configure multiple IPv6 addresses. Each address should have a different prefix so that the switch can be managed from stations on different subnets. When a route to one subnet fails, the switch can be managed from another subnet.

To add a static IPv6 address:

STEP 1 Click **Add**.

STEP 2 Enter an IPv6 address followed by a slash (/) and the prefix length.

STEP 3 Select **EUI-64** if the address conforms to the EUI-64 format, whereby the first three to five octets are the Organizationally Unique Identifier (OUI) and the remaining octets are a unique assigned address.

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

IPv6 Default Router Table

When IPv6 management is enabled, the switch uses the IPv6 neighbor discovery process to identify the default router for communicating with devices outside the local IPv6 subnet. The default router in IPv6 networks is similar in function to the default router in IPv4 networks.

The IPv6 Default Router table lists the default router IP address for each IPv6 management address. A default router address consists of the link-local address of the IPv6 interface on the subnet.

Viewing and Adding IPv6 Neighbors

When IPv6 management is enabled, the switch identifies IPv6-enabled devices on attached links. The switch supports the discovery of up to 1,000 dynamic IPv6 neighbors and supports the static configuration of IPv6 neighbors.

The *IPv6 Neighbors* page lists dynamically discovered and statically configured neighbors, and enables adding static hosts.

To view the IPv6 neighbor Table, click **Administration** > **Management Interface** > **IPv6 Neighbors** in the navigation window.

The IPv6 Neighbor Table displays the following fields for each dynamic entry:

- **IPv6 Address**—IPv6 address of neighbor.
- **MAC Address**—MAC address of the neighbor.
- **State**—State of the neighbor. The following are the states for dynamic entries:
  - **Reachable**—Confirmation was received within a preconfigured interval that the forward path to the neighbor is functioning properly. While in the Reachable state, the device takes no special action as packets are sent.
  - **Delay**—More time has elapsed than a preconfigured interval since the last confirmation was received that the forward path was functioning properly.
- **Age Updated**—The time in seconds that has elapsed since an entry was added to the cache.
- **Type**—Neighbor discovery cache information entry type (static or dynamic).

You can click **Clear Dynamic Neighbors** to clear the table.

Adding Static IPv6 Neighbors

The switch supports up to 16 static IPv6 neighbor entries. To add a static neighbor:

STEP 1 Click **Add**.

STEP 2 Enter an IPv6 global address (not including a prefix length).

STEP 3 Enter the MAC address of the neighbor.

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Managing User Accounts

One management user is configured on the switch by default:

- User Name: **cisco**
- Password: **cisco**

You can use the *User Accounts* page configure up to five additional users and to change a user password.

Adding a User

To add a new user:

STEP 1 Click **Administration** > **User Accounts** in the navigation window.

The User Account Table displays the currently configured users.

STEP 2 Click **Add**.

STEP 3 Enter a user name between 1 to 32 alphanumeric characters. Only numbers 0-9 and letters a-z (upper or lower) are allowed for user names.

STEP 4 Enter a password between 0 and 64 characters (depending upon the **Password Strength** setting) and confirm the password.

As you enter a password, the number and color of vertical bars changes to indicate the password strength, as follows:

- Red—The password fails to meet the minimum complexity requirements. The text “Below Minimum” displays to the right of the meter.
- Orange—The password meets the minimum complexity requirements but the password strength is weak. The text “Weak” displays to the right of the meter.
- Green—The password is strong. The text “Strong” displays to the right of the meter.

If **Password Strength Enforcement** is enabled, **Apply** is not available until the strength meter is orange and the password is confirmed.

When adding a user, you can temporarily disable the password strength check to allow configuring a password that does not meet the strength check criteria. Click **Disable Password Strength Enforcement** and then click **OK** when the warning displays.

To disable the **Password Strength Enforcement** for all users, or to configure its characteristics, use the *Password Strength* page.

STEP 5 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Changing a User Password

To change a user password:

STEP 1 Click **Administration** > **User Accounts** in the navigation window.

STEP 2 Select the user to configure and click **Edit**.

STEP 3 Enter a password between 0 and 64 characters (depending upon the **Password Strength** setting) and confirm the password.

As you enter a password, the number and color of vertical bars changes to indicate the password strength, as follows:

- Red—The password fails to meet the minimum complexity requirements. The text “Below Minimum” displays to the right of the meter.
- Orange—The password meets the minimum complexity requirements but the password strength is weak. The text “Weak” displays to the right of the meter.
- Green—The password is strong. The text “Strong” displays to the right of the meter.

If **Password Strength Enforcement** is enabled, **Apply** is not available until the strength meter is orange and the password is confirmed.

When adding a user, you can temporarily disable the password strength check to allow configuring a password that does not meet the strength check criteria. Click **Disable Password Strength Enforcement** and then click **OK** when the warning displays.

To disable the **Password Strength Enforcement** for all users, or to configure its characteristics, use the *Password Strength* page.

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Deleting a User

You can delete all users except the default user, typically the **cisco** user ID.

To delete a user, select the user name in the User Accounts Table and click **Delete**.

Enabling Management Services

Use the *Management Services* page to enable and disable the available types of management connections. By default, HTTP access is enabled.

Configuring the Idle Session Timeout

The software automatically logs users off the management interface when there is no activity for a specified period of time. The user must reauthenticate after a timeout. You can use the *Idle Session Timeout* page to configure the timeout period.

To configure the timeout period:

STEP 1 Click **Administration > Idle Session Timeout** in the navigation window.

STEP 2 Specify the parameter:

- HTTP Session Timeout—The inactivity timeout for HTTP sessions. The value must be in the range of 1 to 60 minutes. The default value is 10 minutes.

STEP 3 Click **Apply**. Your changes are saved to the Running Configuration.

Login Sessions

The *Login Sessions* page displays active management login sessions. To display this page, click **Administration** > **Login Sessions** in the navigation window.

The page lists the following information for each user currently logged in:

- **ID**—A system-generated ID for the login session.
- **User Name**—Name that the user used to log in.
- **Connection From**—IP address of the host.
- **Idle Time**—Time that has elapsed since the last activity from this user.
- **Session Time**—Amount of time that has elapsed since this user logged in.
- **Session Type**—Protocol in use for the management session (HTTP).

- **Authentication Method**—Lists the protocol used to authenticate the session login. It can be Radius, Local, or None.

Login History

You can use the *Login History* page to display data on previous logins to the management software. To display this page, click **Administration** > **Login History** in the navigation window.

This page displays the following fields:

- **Login Time**—Date and time the user logged in.
- **User Name**—Name that the user used to log in.
- **Protocol**—Protocol the user is using to the configuration software, which can be HTTP, Telnet, Serial, SSH, or SNMP.
- **Location**—IP address of the host.

Time Settings

A system clock is used to provide a network-synchronized time-stamping service for switch software events such as message logs. You can configure the system clock manually or configure the switch as a Simple Network Time Protocol (SNTP) client that obtains the clock data from a server.

See the following topics for information on the configuration pages available in the Administration > Time Settings menu:

- **Setting System Time**
- **Configuring the SNTP Setting**
- **Configuring SNTP Authentication**

Setting System Time

Use the *System Time* page to set the system time manually or to configure the system to acquire its time settings from an SNTP server. To display this page, click **Administration** > **Time Settings** > **System Time** in the navigation window.

By default, the time is configured locally on the switch.

NOTE The actual system time, date, time zone information, and daylight savings time status appears at the bottom of the page.

Specifying Clock Settings Locally

To configure the time settings locally:

STEP 1 On the *System Time* page, select **Use Local Settings**.

STEP 2 Select **Timezone Source - DHCP** if you want to have the switch to acquire its timezone from a DHCP server.

STEP 3 Select **Set Date/Time from Computer** to have the switch retrieve the time settings from the computer you are using to access the switch.

Or clear this field and configure the following time settings:

- **Date**—Enter the date in mm/dd/yyyy format, such as 01/01/2010 for January 1, 2010.
- **Local Time**—Enter the current time in HH:mm:ss format, such as 22:00:00 for 10 p.m. (The hint text displays **HH** if the time is based on a 24-hour clock or **hh** if the time is in 12-hour clock format.)
- **GMT Time Zone Offset**—Select the number of hours and minutes difference between the local time zone and Greenwich Mean Time (GMT).

STEP 4 In the **Time Zone Acronym** field, specify an optional acronym up to four characters to identify the configured settings. This field is for reference only.

STEP 5 Select **Daylight Saving** to configure Daylight Savings Time (DST) settings, if applicable to your time zone. When selected, configure the following fields:

- **USA/European/Other**—Select USA or European to have the DST offset configured to the values used in those locations. Or select **Other** to configure the settings manually. When configuring manually, you can configure the settings for the upcoming DST period only, or you can configure recurring settings.
- **DST Time Zone Acronym**—Specify an optional acronym up to four characters to identify the configured settings. This field is for reference only. (The characters ', ", %, and ? are not supported.)
- **Daylight Savings Offset**—Specify the number of minutes to move the clock forward when DST begins.
- **From/To**—Specify the date and time when DST starts and ends.
- **Recurring**—Select to specify recurring DST periods by selecting the day of the week and number of weeks into the year when DST begins and ends each year.

STEP 6 Click **Apply**. Your changes are saved to the Running Configuration.

Configuring the Switch as an SNTP Client

You can also configure the switch to acquire time from an SNTP server by configuring the switch SNTP Settings.

To configure the switch to acquire time settings from an SNTP server:

STEP 1 On the *System Time* page, select **Use SNTP Server**.

STEP 2 Configure the SNTP client operation mode of the switch:

- **Unicast**—Configures the switch to send unicast SNTP requests to configured unicast SNTP servers only. You must add at least one unicast SNTP server to enable this feature. (Default SNTP servers require that Unicast is selected.)
- **Broadcast**—Configures the switch to get its time settings from SNTP messages broadcast from SNTP servers.

STEP 3 Select **Timezone Source - DHCP** if you want to have the switch to acquire its timezone from a DHCP server.

STEP 4 Configure the **GMT Time Zone Offset** by selecting the number of hours and minutes difference between the local time zone and Greenwich Mean Time (GMT), and specify a **Time Zone Acronym**.

NOTE: If the Timezone Source - DHCP setting is enabled and time zone information is received from the DHCP server, then that information will be used to adjust instead of the manually configured GMT Time Zone Offset and Acronym.

STEP 5 Configure the Daylight Savings Time settings, as described in step **5** in *Specifying Clock Settings Locally*.

STEP 6 Click **Apply**. Your changes are saved to the Running Configuration.

STEP 7 Use the **Configuring the SNTP Setting** and **Configuring SNTP Authentication** to configure additional SNTP settings, such as polling intervals, unicast server addresses, and authentication information the switch needs to access SNTP servers.

Configuring the SNTP Setting

The switch supports the Simple Network Time Protocol (SNTP). SNTP ensures accurate network device time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The switch operates as an SNTP client only and cannot provide time services to other systems.

To display the *SNTP Setting* page, click **Administration** > **Time Settings** > **SNTP Setting** in the navigation window.

Configuring the SNTP Setting

STEP 1 Ensure that the Use SNTP Server option is selected on the *System Time* page and that the Unicast or Broadcast mode is selected as required.

STEP 2 On the *SNTP Setting* page, configure the following:

- **Client Port**—The logical port number to use for the SNTP client on the switch. The default is the well-known IANA port number for this service, 123.
- **Unicast Poll Interval**—The relative rate at which the switch sends synchronization messages to the SNTP server. This field is editable only when SNTP Unicast reception is selected. Enter a value from 3 to 16. The default value is 3. The actual interval, in seconds, is the specified value to the power of 2; for example, if you enter 4, the poll interval is 16 seconds.
- **Broadcast Poll Interval**—The relative rate that the switch broadcasts synchronization messages. This field is editable only when SNTP Broadcast reception is selected. Enter a value from 3 to 16. The default value is 3. The actual interval, in seconds, is the specified value to the power of 2; for example, if you enter 4, the poll interval is 16 seconds."

  If the switch detects a server, it ignores time broadcasts from other SNTP servers unless the Broadcast Poll Interval expires three consecutive times without an update received from the server.

STEP 3 Click **Apply**. Your changes are saved to the Running Configuration.

Adding and Modifying SNTP Servers

The Unicast SNTP Servers Table displays the following information for each SNTP server that you configure:

- **SNTP Server**—IP address or hostname of the SNTP server.
- **Authentication Key ID**—Encryption key required to communicate with the SNTP server.
- **Last Attempt Time**—The time of the most recent attempt by the switch to synchronize with an SNTP unicast server.
- **Status**—Operating status of the SNTP server. Possible values are:
  - **Success**—Client could get the time from this server.
  - **Request timed-out**—Client request timed out.
  - **Bad Date Encoded**—A bad date format was received from server.
  - **Version Not Supported**—Server does not support the SNTP version configured on the switch.
  - **Server Unsynchronized**—Switch time is not synchronized with the server.

  - **Server Kiss of Death**—SNTP server has replied with a kiss of death packet, instructing the switch to stop sending requests to the server, due to traffic spikes or other error conditions.
  - **Other**—The status could not be determined.
- **Last Response**—Time of the last response from the SNTP server.
- **Version**—SNTP protocol version the server uses.
- **Port**—Protocol port number (123 is a well-known port number for SNTP).
- **Polling Mode**—Whether the switch is configured to send SNTP requests to this server (Enabled or Disabled).
- **Total Unicast Requests**—The total number of synchronization requests the switch has made to the unicast server.

To edit the settings for a server, check the box to select it, and then click **Edit**. To remove a server, check the box to select it, and then click **Delete**. To add a new server, click **Add**, and then enter the settings, as described below.

To add an SNTP server:

STEP 1 Click **Add**.

STEP 2 Enter the parameters:

- **SNTP Server**—Enter an IPv4 address or a domain name. To use a domain name, ensure that the DNS service is enabled on the switch (see **Domain Name System**).
- **Authentication Key**—Select **Enable** if authentication is needed when communicating with the SNTP server.
- **Authentication Key ID**—If authentication is used, select the Authentication Key ID from the list. See **Configuring SNTP Authentication** for information on configuring authentication keys.
- **Polling Mode**—Select **Enable** to allow the switch to send requests to this server.

- **Port**—Specify the UDP port number to be specified in the SNTP message headers. By default, the port number is the well-known IANA value of 123.
- **Version**—Specify the highest SNTP version (1–4) that the server supports.

STEP 3 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Viewing Active Server Properties and Global Parameters

The *SNTP Setting* page displays the following properties for the SNTP server, if any, from which the switch most recently acquired its time settings. This page also displays global (nonconfigurable) parameters.

Active Server:

- **Server Host Address**—IP address of the SNTP server.
- **Server Type**—IP protocol version the server uses (IPv4 or IPv6).
- **Server Stratum**—Hierarchical level of the SNTP server that identifies its distance from a reference clock.
- **Server Reference Id**—32-bit code that identifies the reference clock that this server uses.
- **Server Mode**—Mode in which the server is operating:
  - **Unicast**—The SNTP server listens to unicast requests from SNTP clients.
  - **Broadcast**—The SNTP server sends broadcast messages periodically to SNTP clients.
  - **Reserved**—No reply has been received from an SNTP Server. When a response is received from a server, it is overwritten with one of the valid states (Broadcast or Unicast).

Global Parameters:

- **SNTP Client Version**—The highest SNTP protocol version supported by the switch.
- **Last Update Time**—The time of receipt of the most recent SNTP update.

- **Last Unicast Attempt Time**—The time of the most recent attempt by the switch to synchronize with an SNTP unicast server.
- **Client Mode**—The configured SNTP client mode (Unicast or Broadcast). See the *System Time* to configure this mode.
- **Server Maximum Entries**—Maximum number of servers that you can configure on the switch.
- **Server Current Entries**—Number of SNTP servers currently configured on the system, as listed in the Unicast SNTP Servers Table.
- **Broadcast Count**—Number of SNTP broadcast packets that the switch has received from SNTP servers.

Configuring SNTP Authentication

Use the *SNTP Authentication* page to configure encryption keys, which contain the identifying information that the switch uses to authenticate to STNP servers. You also use this page to enable the SNTP authentication service.

When you define SNTP servers that the switch can use, you specify whether a server uses authentication and which authentication key it uses.

NOTE You must configure at least one trusted authentication key before you enable SNTP authentication. Otherwise, the **`Failed to enable SNTP Authentication`** message displays.

To configure an authentication key and enable this service:

STEP 1 Click **Administration** > **Time Settings** > **SNTP Authentication** in the navigation window.

The SNTP Authentication Table displays each currently configured authentication key and whether the key is currently enabled for use as a trusted key.

STEP 2 Select **Enable** to require the switch to authenticate to an SNTP server before synchronizing its time.

STEP 3 Click **Apply**. Your changes are saved to the Running Configuration.

STEP 4 In the SNTP Authentication Table, click **Add** to add a key to the list.

STEP 5 Enter the parameters:

- **Authentication Key ID**—The key number. When you define an SNTP server on the system, you specify which key it uses for authentication.
- **Authentication Key**—The value of the key. The value is the cryptographic key that is used to encrypt and decrypt SNTP messages to and from the server.
- **Trusted Key**—Indicates whether this key is a trusted key. Only trusted keys are available for use. At least one trusted key must be configured to enable the SNTP authentication service.

  Keys are used with unicast SNTP servers only. A key is used to authenticate an SNTP server only when the key is enabled as trusted. A keys that is configured on the switch but specified as untrusted will not be used. An administrator can add an untrusted key to have it available for use at another time.

STEP 6 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

System Logs

The switch generates messages in response to events, faults, errors, changes in the configuration, and other occurrences. These messages are stored locally in the system memory and are forwarded to one or more centralized points of collection for monitoring or long-term archiving.

See the following topics for more information on the configuration pages available in the Administration > System Log menu:

- **Configuring Log Settings**
- **Configuring Remote Log Servers**

Configuring Log Settings

Use the *Log Settings* page to enable logs globally, and to define which event types are logged into temporary memory (RAM) and persistent memory (flash).

Log messages in flash memory are retained across a reboot. When the log is full, the oldest events are automatically deleted and replaced with the new entries.

To configure log settings:

STEP 1 Click **Administration** > **System Log** > **Log Settings** in the navigation window.

STEP 2 Enable the types of logging to be performed on the system:

- **Log Aggregation**—When enabled, this feature combines multiple logs of the same type into a single log message. If two or more identical log messages are received consecutively within a configured time interval, then these messages are aggregated into a single log message.
- **Log Aggregation Interval**—If Log Aggregation is enabled, specify the interval in seconds. Consecutive messages that are received within this interval will be aggregated into a single log message. The range is 15 seconds to 120 seconds.
- **RAM Memory Logging**—Select to enable logging in RAM.
- **Flash Memory Logging**—Select to enable logging in flash memory.
- **Flash Log Size**—Enter the maximum number of log messages to store in the flash memory log.

STEP 3 Enable the event severity levels to be logged for each log type. The severity levels are listed from the highest 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.

NOTE: When you select a severity level, any events of that level or higher are automatically selected for logging.

STEP 4 Click **Apply**. Your changes are saved to the Running Configuration.

Configuring Remote Log Servers

You can define one or more remote log servers that the switch sends Syslog messages to. Use the *Remote Log Servers* page to define log servers and to set the severity level of the log events to be sent to the server.

To enable Syslog operation and configure a remote log servers:

STEP 1 Click **Administration** > **Remote Log Servers** in the navigation window.

STEP 2 For the Syslog Logging mode, click **Enable**, and then configure the following settings:

- **Facility**—Select a value from the list that identifies the classification of syslog messages from this switch. The meaning of these values (Local 0 through Local 7) is determined by the network administrator.
- **Local Port**—Specify the IANA port number for the switch. The default is the well-known port number for the Syslog protocol, 514.

STEP 3 Click **Apply**.

STEP 4 In the Remote Log Server Table, click **Add**.

STEP 5 Enter the parameters:

- **Log Server**—IPv4 address or hostname of the server to send logs to.
- **UDP Port**—The logical UDP port number the remote server uses for the Syslog protocol. The default value is the well-known IANA Syslog port number, 514.
- **Minimum Severity**—Only items that meet or exceed this severity level are sent to the remote server. See **Configuring Log Settings** for a description of the severity levels.

STEP 6 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

File Management

You can use the file management features to upgrade or backup the firmware, update the language files, save configuration changes, copy configuration files within the switch, and set up autoconfiguration feature.

NOTE When any download or upload to or from the switch is in progress, all management access to the switch is blocked until the transfer is complete to protect the switch from any unknown changes.

NOTE When logging in by using HTTP/HTML, and you can choose from more than one network port, you should the lowest number port.

See the following topics for more information on the configuration pages available in the File Management menu:

- **Upgrading and Backing Up Firmware and Language Files**
- **Downloading and Backing Up the Configuration and Log Files**
- **Delete Configuration**
- **Copying and Saving Configuration Files**
- **DHCP Auto Configuration**
- **Firmware Recovery Over HTTP**
- **Downloading an Image or Boot Code File From the System Boot Prompt**

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 another file type, such as the Startup Configuration, to be preserved after a reboot.

  If the switch is rebooted, the Running Configuration is lost. When the switch is rebooted, the Startup Configuration stored in the Flash is copied to the Running Configuration stored in RAM.

- **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 Running Configuration, created by the switch after:

  - The switch has been operating continuously for 24 hours.
  - Configuration changes have been made to the Running Configuration in the previous 24 hours, but have not been saved.

  Only the switch can copy the Running Configuration to the Mirror Configuration. However, you can copy from the Mirror Configuration to other file types or to another device.

- **Firmware**—The operating system. 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.
- **Operational Log**—Events that are not saved to the Startup Log.
- **Startup Log**—The first 32 messages logged when the switch is booted. Subsequent messages are logged into the Operational Log. The Startup Log is not aged out; it retains the messages until the switch is rebooted.
- **Trap Log**—SNMP traps.
- **SSH Files**—Encryption keys used for secure shell communication.

Upgrading and Backing Up Firmware and Language Files

You can use the *Upgrade/Backup Firmware/Language* page to:

- Upgrade the firmware by downloading a new image from a server.
- Upgrade the boot code by downloading a new boot file from a server.
- Update the language files by downloading a new file from a server. Language files determine the language options for the web-based switch configuration utility. You can select the display language when you log in.
- Back up the firmware image to a server.

English is always the default language.

NOTE You can also back up or restore the configuration files. See **Downloading and Backing Up the Configuration and Log Files** for more information.

To upgrade or backup the firmware or to update the boot code or language file:

STEP 1 Click **Administration** > **File Management** > *Upgrade/Backup Firmware/Language* in the navigation window.

STEP 2 Enter the parameters:

- **Transfer Method**—Select the protocol to be used for the file transfer (TFTP or HTTP), which corresponds to the type of server you are downloading to or uploading from.
- **Save Action**—Select **Upgrade** to download a file to the switch, or select **Backup** to copy a file from the switch to the server.
- **File Type**—Select the type of file to upgrade or back up (you can back up only the firmware image):
  - **Firmware Image**—Controls all switch features and interfaces.
  - **Boot Code**—Controls the initial system bootup.
  - **Language File**—Strings used by the system interface to display the selected language.
- **TFTP Server** (TFTP only)—Specify the IPv4 or IPv6 address of the TFTP server. Or specify the server name if DNS is enabled in the IP configuration (see Domain Name System).
- **Source File Name**—For upgrades via TFTP, enter the filename, including the path. For upgrades via HTTP, browse and select the file from your computer.
- **Destination File Name**—For backups via TFTP, enter the filename, including the path. This field does not appear for backups via HTTP.

STEP 3 Click **Apply** to begin the upgrade or backup. A progress bar indicates the status of the file transfer. A typical image transfer might take 5-6 minutes to complete.

STEP 4 Reboot the switch to use the new configuration or firmware.

WARNING Ensure that power to the switch remains uninterrupted while downloading an image or a boot code file to the switch. If a power failure occurs while downloading a file, the file contents in persistent memory are lost.

If a power outage occurs during boot code file download, the switch will not be able to boot. Contact the Cisco Small Business Support Center for assistance.

If a power outage occurs during image download, the image will not load, but the boot loader will continue to be operational. See **Firmware Recovery Over HTTP** for instructions on downloading a working image.

Downloading and Backing Up the Configuration and Log Files

You can use the *Download/Backup Configuration/Log* page to download a saved configuration file to the switch to restore previously saved settings, or back up the current configuration file to a network location. You also can use this page to back up log files.

- **Downloading a Configuration File to Restore Settings**
- **Backing Up the Configuration File and Logs**

Downloading a Configuration File to Restore Settings

To download a configuration file to the switch to restore a previously backed-up file:

STEP 1 Click **Administration** > **File Management** > **Download/Backup Configuration/Log** in the navigation window.

STEP 2 Select the **Transfer Method** (HTTP or TFTP).

STEP 3 For the **Save Action**, select **Upgrade** to download the file that will be specified below.

STEP 4 Enter the following parameters:

- **TFTP Server** (TFTP only)—Specify the IPv4 or IPv6 address of the TFTP server. Or specify the server name if DNS is enabled in the IP configuration (see Domain Name System).
- **Source File Name**—For TFTP, specify the filename, including the path. For HTTP, browse to select the file from your computer.
- **Destination File Type**—Select one of the following options:
  - **Startup Configuration**—If the specified configuration file is valid, then it will replace the current Startup Configuration file. It will be the active configuration file when you reboot.
  - **Backup Configuration**—The specified file will replace the current backup configuration file.

STEP 5 Click **Apply** to begin the upgrade. A progress bar indicates the status of the upgrade.

CAUTION Ensure that power to the switch remains uninterrupted while the configuration file is downloading to the switch. If a power failure occurs while downloading the configuration file, the file is lost and the process must be restarted.

Backing Up the Configuration File and Logs

To back up the configuration file or log:

STEP 1 Click **Administration** > **File Management** > **Download/Backup Configuration/Log** in the navigation window.

STEP 2 Select the Transfer Method (HTTP or TFTP).

STEP 3 For the **Save Action**, select **Backup**.

STEP 4 Enter the parameters:

- **TFTP Server** (TFTP only)—Specify the IP address of the TFTP server. Or specify the server's domain name if DNS is enabled in the IP configuration (see Domain Name System).
- **Destination File Name** (TFTP only)—Specify a name for the saved file, including the path on the TFTP server.
- **Source File Type**—Select the configuration file type:
  - **Running Configuration**—The current configuration, including any changes applied in the current management session.
  - **Startup Configuration**—The configuration file saved to flash memory. This file does not include any configuration changes applied in RAM but not yet saved to the switch.
  - **Backup Configuration**—An additional configuration file saved on the switch for use as a backup. The administrator can copy the Backup Configuration file to the Startup Configuration file type, then reboot the switch to use the Backup Configuration file.
  - **Mirror Configuration**—If the Running Configuration is not modified for at least 24 hours, it is automatically saved to a Mirror Configuration file type, and a log message with severity **alert** is generated to indicate that a new mirror file is available. This feature allows the administrator to view the previous version of the configuration before it is saved to the Startup Configuration file type or to copy the Mirror Configuration file type to another configuration file type. If the switch is rebooted, the Mirror Configuration is reset to the factory default parameters.
  - **Flash Log**—Log of events saved to flash memory.
  - **Operational Log**—Log of events in switch RAM but not saved to flash memory.
  - **Startup Log**—The first 32 messages logged when the switch is booted. Subsequent messages are logged into the Operational Log.

STEP 5 If you are backing up the Operational Log or Startup Log, select the Log Version to back up.

The switch maintains three versions of each log. The Version 1 log is the current or most recently created log file, the Version 2 log is the next most recent, and the Version 3 log is the oldest.

STEP 6 Click **Apply**.

For HTTP backups, you are prompted to browse to a location to save the file. A progress bar indicates the status of the file transfer.

Delete Configuration

The *Delete Configuration* page enables you to delete the Startup configuration or the Backup configuration. If you delete both the startup and the backup configuration files, when the switch reboots it will use the default configuration file.

To delete the Startup or Backup Configuration file:

STEP 1 Click **Administration** > **File Management** > **Delete Configuration** in the navigation window.

STEP 2 Select the Startup Configuration or Backup Configuration file type.

STEP 3 Click **Apply**.

Copying and Saving Configuration Files

The *Copy/Save Configuration* page enables you to copy files within the file system. For example, you can copy the Backup Configuration file to the Startup Configuration file so that it will be used the next time you boot up the switch.

To copy a file to the Startup or Backup Configuration file:

STEP 1 Click **Administration** > **File Management** > **Copy/Save Configuration** in the navigation window.

STEP 2 Select the Source File Name:

- **Running Configuration**—Current configuration, including any changes applied in the current management session.
- **Startup Configuration**—Configuration file type used when the switch last booted. This does not include any configuration changes applied but not yet saved to the switch.
- **Backup Configuration**—Backup configuration file type saved on the switch.
- **Mirror Configuration**—If the Running Configuration is not modified for at least 24 hours, it is automatically saved to the Mirror Configuration file type, and a log message with severity level **Alert** is generated to indicate that a new Mirror Configuration file is available. The Mirror Configuration file can be used when the switch has problems booting with the Startup or Backup Configuration file types. In such cases, the administrator can copy the Mirror Configuration to either the Startup or Backup Configuration file type and reboot.

STEP 3 For the Destination File Name, select the file type to be overwritten with the file you are copying:

- **Startup Configuration**—Configuration file type used when the switch last booted. This does not include any configuration changes applied but not yet saved to the switch.
- **Backup Configuration**—Backup configuration file type saved on the switch.

STEP 4 Click **Apply** to begin the copy process.

When complete, a window displays the message, Copy Operation Successful.

DHCP Auto Configuration

The switch supports Auto Configuration through DHCP to facilitate configuration deployment and upgrades. This feature enables the configuration of a switch automatically when no configuration file is found in device storage during the boot process or when a newer configuration file is available for download.

NOTE The Auto Configuration feature depends upon the proper configuration of other devices in the network, including a DHCP or BOOTP server, a TFTP server, and if necessary, a DNS server.

Overview

During startup, the switch attempts communication with a DCHP server to obtain its IP address and other information. If Auto Configuration is enabled, the switch may also download a startup configuration file, depending on the TFTP server and startup configuration file name it receives from the DHCP server. Auto Configuration is enabled by default.

DHCP Auto Configuration initiates when the switch is rebooted with Auto Configuration enabled, and any of the following conditions occur:

1. Information on the TFTP server and Startup Configuration is received from the DHCP server, and Auto Configuration has not previously downloaded the configuration file.
2. Information on the TFTP server and Startup Configuration is received from the DHCP server, and the configuration file name differs from the file name advertised in a previous DHCP message.
3. The Startup Configuration file is not present and no information on the TFTP server or Startup Configuration is received from the DHCP server.

When conditions 1 and 2 occur, the switch saves the file to flash memory. Upon subsequent startups, it compares the stored file name to the name specified in option 66/67 in the current DHCP message. If they differ, the new file is downloaded and written to flash memory.

NOTE When the system boots up for the first time, the switch does not have a specific name for the configuration file received from the DHCP server, as it has not downloaded a Startup Configuration file yet. If these options are received in the DHCP message, then that file name is saved and the download process begins.

When option 3 occurs, the switch looks for the TFTP server and Startup Configuration file as described in **Default Network Configuration File**.

DHCP Server Message Details

Any of the following fields might be returned by a BOOTP or DHCP server and processed by the switch:

- The name of the configuration file (boot file or option 67) to be downloaded from the TFTP server.
- The identification of the TFTP server from which to obtain the boot file.

  The TFTP server IP address can be deduced from the multiple sources in a DHCP reply. The switch makes its selection based on the following criteria, from the highest priority to the lowest:

1. The **sname** field in a DHCP or BOOTP reply.
2. The TFTP server name (option 66) field in a DHCP reply.
3. The TFTP server address (option 150) field in a DHCP reply.
4. The siaddr field of a DHCP or BOOTP reply.

If only the sname or option 66 values are returned to the switch, a DNS server is needed to resolve the IP address of the TFTP server. After an IP address is assigned to the switch, if a hostname is not already assigned, Auto Configuration sends a DNS request for the corresponding hostname.

Alternate TFTP Server and File Name

On the *DHCP Auto Configuration* page, you can configure an alternate TFTP server and file name to be used when the server or file name provided by the DHCP server cannot be located. The following procedure is followed:

1. The switch sends unicast messages to the TFTP server identified through DHCP, if provided.
2. If the DHCP information is not provided or the server or file name cannot be found, then the server uses the alternate information, if configured.
3. If the alternate information is not configured or the server or file name cannot be found, the switch sends broadcast TFTP requests for the file name in the DHCP message, if given. Otherwise, the switch enters default network configuration mode process described in the **Default Network Configuration File** section.

Configuration File Download Details

The switch first attempts to download a host-specific configuration file. If this is not possible, it downloads the configuration file *<hostname>*.cfg if Default Network Configuration Mode is enabled.

Host-specific Configuration File

The switch attempts to download the host specific configuration file whose name is specified as the boot file name in the reply from a DHCP/BOOTP server, or is configured as the Backup Configuration File for DHCP Auto Configuration. The switch makes three unicast TFTP requests for the specified boot file. If the unicast attempts fail, or if a TFTP server address was not provided, the switch makes three broadcast requests to any available TFTP server for the specified boot file. When the switch gets the configuration file, the configuration is validated for errors. If the validation is successful, the switch copies the configuration to the Startup Configuration file type, stores the configuration file name in non-volatile memory, and reboots the unit.

NOTE The switch requires the boot file name to have a *.cfg* extension.

Default Network Configuration File

If Default Network Configuration Mode is enabled, the switch downloads the configuration file <*hostname*>.cfg when any one of the following conditions occurs:

- A host specific configuration file is not specified or configured.
- A host specific configuration file does not exist on the TFTP server.
- A failure occurs during the download.

NOTE The startup configuration file cannot be present on the switch. If the startup configuration file is present on the switch, this process is not initiated.

To resolve the hostname in the configuration file, the switch first downloads fp-net.cfg from the TFTP server. The fp-net.cfg file is referred as the default network configuration file and contains one or more IP-address-to-host-name mappings. The switch determines the hostname from the mappings with its IP address. If there is no mapping, the switch uses reverse DNS lookup to discover the hostname.

The following is a sample fp-net.cfg file.

```
config
  ...
  ip host switch_to_setup 192.168.1.10
  ip host another_switch 192.168.1.11
  ... <other hostname definitions>
exit
```

When a hostname has been determined, the switch issues a TFTP request for a file named <*hostname*>.cfg, where <*hostname*> is the first eight characters of the switch hostname.

The switch uses the IP address to do a DNS reverse name lookup. For example, if the switch IP address is 192.168.1.10, the hostname becomes **switch_t.cfg** (the first eight characters in the example above).

The default switch name is derived as **switch**+*last 6 digits of hex address*. The mapping file should have the hostnames such as **ip host switchD99FA5 192.168.1.10**. Then, the hostname learned for the <*hostname*.cfg> is **switchD9.cfg** for the switch having the IP address **192.168.1.10**.

If the switch is unable to map its IP address to a hostname, Auto Configuration sends TFTP requests for the default configuration file **host.cfg**.

When the switch gets the default configuration file, the configuration is validated for errors. If the validation is successful, then the switch copies the configuration to the Startup Configuration file type and reboots. In this case, the default configuration file name is not stored in the non-volatile memory.

NOTE If the switch is unable to get the valid configuration file, then the process described above is repeated every 20 minutes until the switch gets a valid configuration file. The administrator can create a Startup Configuration file by manually saving the Running Configuration. The administrator can also disable Auto Configuration if desired.

The following table summarizes the configuration files that can be downloaded, and the order in which they are sought.

Order Sought	File Name	Description	Final File Sought
1	<bootfile>.cfg	Host-specific configuration file, ending in a *.cfg file extension[1]	Yes
2	fp-net.cfg	Default network configuration file	No
3	<hostname>.cfg	Host-specific configuration file, associated with hostname	Yes
4	host.cfg	Default configuration file	Yes

1. This file name might be learned through DHCP or manually configured, as described in **Alternate TFTP Server and File Name**.

An operator can terminate Auto Configuration at any time prior to the downloading of the file. This should be done when the switch is disconnected from the network, or if the required configuration files have not been set up on TFTP servers.

When a configuration file is successfully downloaded and saved to the Startup Configuration file type, the switch logs a message with severity level Alert prior to rebooting.

Setting DHCP Auto Configuration

You can use the *DHCP Auto Configuration* page to enable and disable the feature, configure TFTP server and file name settings, and view status information.

When DHCP Auto Configuration is enabled, it will be in the **Waiting for boot options** state, until it receives the notification from the DHCP client. The DHCP client triggers the Auto Install process when it receives the IP address from the DHCP server, after which the status changes to **Processing DHCP/BOOTP options, checking preconditions**.

The following messages might display:

- `Waiting for boot options`
- `Processing DHCP/BOOTP options, checking preconditions`
- `Downloading tftp://<tftp address>/<filename>`
- `Applying downloaded configuration`
- `Waiting for restart timeout`
- `Saving the downloaded configuration`
- `Stopped`
- `AutoInstall is completed.`
- `AutoInstall process is terminated:File <filename> validation failed.`
- `AutoInstall process is terminated:Failed to save the downloaded configuration file<bootfile> to start-up configuration.`
- `AutoInstall process terminated:Startup config is created manually.`
- `AutoInstall process is terminated :Boot file matched with the last downloaded file.`
- `AutoInstall process is terminated:Failed to resolve the boot file name.`

To configure DHCP Auto Configuration:

STEP 1 Click **Administration** > **File Management** > **DHCP Auto Configuration** in the navigation window.

STEP 2 Enter the parameters:

- **Auto Configuration Via DHCP**—Select **Enable** to enable this feature on the switch.
- **Default Network Config Mode**—Select Enable to have the switch download a default configuration file named *fp-net.cfg* when no host-specific file is found on the switch. See **Default Network Configuration File** for details.
- **Alternate TFTP Server**—Specify the IP address of a TFTP server to serve as a backup. An alternate TFTP server is used when unicast requests to the TFTP server specified in option 66 fails three times. (The length of the string cannot exceed 96 characters.)
- **Alternate Configuration File**—Specify an alternate configuration file name to serve as a backup. If no startup configuration file identified in DHCP option 67, or if the specified file cannot be found on the TFTP server, Auto Configuration looks for the alternate file name. (The length of the string cannot exceed 32 characters.)
- **Last Auto Configuration File Name**—The configuration file name used the last time the Auto Configuration process executed. If a different file name is identified through DHCP, the file download process will begin.
- **Current Status**—The status of the Auto Configuration process. Possible values are **AutoInstall Complete** or **In Progress**.

STEP 3 Click **Apply**. Your changes are saved to the Running Configuration.

Firmware Recovery Over HTTP

The switch has a firmware recovery feature that enables the restoration of a valid image on the switch after a failed download. If the power goes down during an image download, the switch might not be able to boot. In this event, although the image is not usable, the boot loader file that loads the firmware image from Flash memory to RAM should continue to be functional. An HTTP server is embedded in the boot loader file, enabling the administrator to connect to the switch over a switch port and use a web browser to download and install a new firmware image.

The switch enters the HTTP firmware recovery mode when the switch is booted and the boot loader cannot find a valid image in flash memory. In this mode, the boot loader sets the switch internal network port to the following static IP address:

- IP Address: 192.168.1.254
- Network Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

An HTTP server starts and listens for client connections on port 80.

NOTE Firmware recovery can also be performed using the command line interface. Refer to the *Cisco Small Business SF200E Command Line Reference*.

To use this feature to download a new firmware image:

STEP 1 Directly connect a management PC to any switch port.

STEP 2 Configure the IP address and mask on the management PC to be in the same subnet as the switch.

NOTE: You can access the system across a network if the default gateway IP address is 192.168.1.1.

STEP 3 Open a web browser and enter the IP address of the switch in the address bar (192.168.1.254).

NOTE: The HTTP firmware recovery features supports the following browsers:

- Firefox 3.0 and later versions
- Internet Explorer 6 and later versions

A Firmware Recovery page displays. No authentication is required.

The web page displays the PIC VID (product ID and vendor ID), serial number, and MAC Address of the switch.

STEP 4 Select **Browse** and select a valid firmware image to download.

A progress bar appears while the file is downloading. The following message appears upon a successful download:

100% Complete
File downloaded successfully. Please wait while the file is being written to flash.

The file selected by administrator is downloaded to RAM and is validated for following conditions:

- The CRC of the file is good.
- The STK file is built for this platform.
- The STK file size is within the partition limits (4.5 MB is reserved for this file).

If these conditions are met, the file is written to Flash memory and the system is rebooted using the new firmware.

If any of these checks fail, the image is not written to Flash memory and the recovery process is stopped. You can restart the recovery process with a correct image file.

If the transfer is aborted because the browser window is refreshed or closed, the session is cleared and the session times out immediately. If the transfer is aborted because the network is unreachable, the session times out after 45 seconds. After the session times out, you can begin the recovery process again.

Downloading an Image or Boot Code File From the System Boot Prompt

You can download and install a new image or boot code file at the system boot prompt using the TFTP and XMODEM protocols. This process may be necessary when the application software does not execute due to a corrupted software image or boot code file and, as a result, you cannot access the CLI or web-based interface utilities for downloading and installing new software.

If the switch is connected to a network, you can obtain IP information for the switch via DHCP, and then use TFTP to download the file.

If no network connection is available, and the switch is connected through its serial console port to a management station, you can use the XMODEM protocol to download the file.

NOTE This process requires a management system that is connected to the serial console port on the switch and has a terminal emulation program, such as Tera Term or HyperTerminal. Configure the utility with the following parameters:

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

See your product *Quick Start Guide* for more information on setting up the console port connection.

Downloading an Image or Boot Code File Using TFTP

To download a software image or boot code file using TFTP at the boot prompt:

STEP 1 Using a terminal emulation program, open a serial connection between the switch and the management system connected to the switch console port.

STEP 2 Physically connect switch port e1 to the network.

STEP 3 Power up the switch.

STEP 4 Stop the firmware load by pressing and holding <**Ctrl**> + **C** as the switch boots up. The boot-level command prompt displays:

```
CFE>
```

STEP 5 Enter the command to have an IP address assigned to the port from a DHCP server on the attached network:

```
CFE> ifconfig eth0 -auto
```

When the switch receives a DHCP reply, the IP information displays on the terminal.

STEP 6 Enter the command to download an image file to Flash:

```
CFE>flash server-ipaddr:image-filename flash0.os
```

Or, enter the command to download a boot code file:

```
CFE> flash ipaddr:bootcode-filename flash0.boot
```

Replace *ipaddr* with the IP address of the system where the file resides, and replace *image-filename* or *bootcode-filename* with the actual image or boot code filename.

WARNING! Make sure that the switch is connected to an uninterrupted power supply during a boot code upgrade. This process might take 10–20 seconds.

When the download is complete, the switch copies the image or boot code file into Flash memory.

STEP 7 Enter the command to restart the switch to boot it with new software:

```
CFE>reset -sysreset
```

NOTE: You can verify the boot code or image version by viewing the System Summary page in the web-based switch configuration utility. Or, from the command line interface, you can enter the **show sysinfo** command.

Downloading an Image or Boot Code File Using XMODEM

To download a software image or boot code file using XMODEM at the boot prompt:

STEP 1 Using a terminal emulation program, open a serial connection between the switch and the management system connected to the switch console port.

STEP 2 Power up the switch.

STEP 3 Stop the control at boot code by pressing and holding <**Ctrl**> + **C** continuously as the switch boots up, until the following prompt displays:

```
CFE>
```

STEP 4 Enter the command to download a software image:

```
CFE>flash uart0 flash0.os
```

Or, enter the command to download a boot code file:

```
CFE>flash uart0 flash0.boot
```

WARNING! Make sure that the switch is connected to an uninterrupted power supply during a boot code upgrade. This process might take 10–20 seconds.

The switch waits for a file to be sent from the management station.

STEP 5 In the terminal emulation software, select the file and begin the transfer.

For example, in Tera Term, click **File** > **Transfer** > **XMODEM** > **Send**, and then browse to select the file.

When the download is complete, the switch burns the image or boot code file into Flash memory.

STEP 6 Enter the command to restart the switch to boot it with new software:

```
CFE>reset -sysreset
```

NOTE: You can verify the boot code or image version by viewing the System Summary page in the web-based switch configuration utility. Or, from the command line interface, you can enter the **`show sysinfo`** command.

Rebooting the Switch

Use the *Reboot* page reboot the switch. To reboot the switch:

STEP 1 Click **Administration** > **Reboot** in the navigation window.

STEP 2 Select one of the following options:

- **Reboot**—Reboots the switch using the latest save configuration.
- **Reboot to Factory Default**—Reboots the switch using with the factory default configuration file. Any customized settings are lost.

A window appears to enable you to confirm or cancel the reboot. The current management session might be terminated.

STEP 3 Confirm or cancel the reboot.

Pinging Hosts

Use the *Ping* page to send a Ping request from the switch to a specified IP address. You can use this feature to check whether the switch can communicate with a particular network host.

To ping a network host:

STEP 1 Click **Administration** > **Ping** in the navigation window.

STEP 2 Select **IPv4** or **IPv6** as the Address Type.

STEP 3 For an IPv4 address, enter the following parameters:

- **IP Address/Hostname**—Enter the IP address or the hostname of the station you want the switch to ping.
- **Count**—Specify the number of pings to send.
- **Interval**—Specify the number of seconds between pings sent.
- **Datagram Size**—Specify the data size of the ping packet to send.

For an IPv6 address, enter the following parameters:

- **Ping Type**—Select Global to ping an address outside the local subnet. Select Link Local to ping an address on the local subnet.
- **IPv6 Address/Hostname**—(Global addresses only) Enter the 128-bit global address.
- **IPv6 Link-Local Address**—(Link-local addresses only) Enter the link local address if the address is on the same subnet as the switch.
- **Datagram Size**—Specify the data size of the ping packet to send (between 48 and 2048 bytes).

STEP 4 Click **Apply** to send the ping. You can view the status in the Ping window.

Configuring Control Packet Forwarding

You can use the *Control Packet Forwarding* page to configure how the switch handles packets of the following protocol types:

- CDP—The Cisco Discovery Protocol (CDP), which is supported on many types of Cisco networking equipment. CDP enables directly connected devices to share information such as their IP addresses, capabilities, and software versions. Although the switch does not itself support CDP, it can forward CDP packets on behalf of connected devices within a VLAN.
- Dot1X—The IEEE 802.1X protocol defines how Extensible Authentication Protocol (EAP) packets are encapsulated over a LAN. Dot1X provides a way to authenticate users and allow or deny them access to services made available by switch ports. See 802.1X for information on configuring the Dot1X feature on the switch.

- LLDP—Network devices use the Link Layer Discovery Protocol to advertise their capabilities to other devices. See LLDP-MED for information on configuring the LLDP feature on the switch.

To configure control packet forwarding:

STEP 1 Click **Administration** > **Control Packet Forwarding** in the navigation window.

STEP 2 Select the protocol you want to configure (CDP, LLPD, or DOT1x).

STEP 3 Select the action that a port will take when received packets of the specified type:

- **Drop**—All packets of the selected type are dropped.
- **Forward**—All packets of the selected type are forwarded within the specified VLAN. This is the default action for CDP packets.
- **Terminate**—The packet is accepted and processed on the switch. This is the default action for LLDP and DOT1X packets and is not available for CDP packets.

STEP 4 Click **Apply**. Your changes are saved to the Running Configuration.

Diagnostics

You can use the diagnostics pages to perform virtual cable tests for copper and fiber optics cables, set up a diagnostic monitor for a port or VLAN, and to view CPU utilization data.

See the following topics for more information on the configuration pages available in the Administration > Diagnostics menu:

- **Testing Copper Ports**
- **Configuring Port and VLAN Mirroring**
- **CPU/Memory Utilization**

Testing Copper Ports

Use the *Copper Ports* page to perform tests on copper cables. These physical layer diagnostics can be used to help determine where in the cable a break might exist.

The Copper Ports Table lists each port and the following data, which it learned through the most recent test (default data appears if the port has not been tested):

- **Test Result**—Results of the most recent cable test. Possible values are:
  - **Normal**—Cable is working correctly.
  - **Open**—Cable is disconnected or the connector is faulty.
  - **Short**—Cable has an electrical short.
  - **Untested**—No test has been performed.
  - **Cable status test failed**—Cable status could not be determined by the test. The cable might be working.
- **Distance to Fault**—Distance in meters from the port where the cable error, if any, was detected in the most recent cable test.
- **Last Update**—Last time the port was tested.
- **Cable Length**—Length of the cable in meters.

To initiate a copper port test:

STEP 1 Click **Administration** > **Diagnostics** > **Copper Ports** in the navigation window.

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

If the port has an active link while a cable test is run, the link might go down for the duration of the test. It might take several seconds to run the test. When complete, a window appears with the test results.

Configuring Port Mirroring

Use the port mirroring feature to send network traffic on a port copied to another port for analysis by a network analyzer.

A mirroring session consists of a *destination probe port* and at least one *source port*. A mirror copy of the traffic on the source port(s) being probed are transmitted from the source port to the destination probe port. A network analyzer can be connected to a destination probe port to analyze network traffic.

A port configured as a destination probe port acts as a mirroring port as long as the session is operationally active. When the session is not active, the port transmits and receives traffic based on the other configuration parameters.

NOTE When a port is configured as a probe port, the switch does not forward or receive any traffic or respond to a ping.

To display the *Port and VLAN Mirroring* page, click **Administration** > **Diagnostics** > **Port Mirroring** in the navigation window.

Four mirroring sessions are available for configuration and are disabled by default. The Port Mirroring Session Table displays the following fields for each session:

- **Session ID**—A monitoring session ID number.
- **Admin Mode**—Indicates whether the port mirroring session is enabled or disabled.
- **Destination Interface**— To enable this feature, select it and choose the port to where the traffic on the source port is mirrored to the destination probe port.
- **Source Interface**—List of the source interfaces selected to participate in this mirroring session.

The Port Mirroring Source Interface Table lists the source interfaces assigned to each session. You can select Filter and select a Session ID to display data for only one session.

To set up port mirroring, you first assign source interfaces to a session. Then, you define a destination interface and enable the session. A session is operationally active only when the source and destination interfaces are configured and the administrative mode is enabled.

To configure a mirroring session:

STEP 1 In the Port Mirroring Source Interface Table, click **Add**.

STEP 2 Select a Session ID.

STEP 3 Select the Source Interface and the type of traffic to be mirrored.

STEP 4 By using the Type radio button, specify the direction of the traffic at the source interface that is to be monitored:

- **Rx Only**—Incoming traffic
- **Tx Only**—Outgoing traffic
- **Tx and Rx**—Both incoming and outgoing traffic

STEP 5 Click **Apply**. Your changes are saved to the Running Configuration.

You can repeat the process to assign multiple Source Interfaces to the same session. However, a source interface can be used in only one active session at a time.

STEP 6 In the Port Mirroring Session Table, select the session to activate and click **Edit**.

STEP 7 For the Admin Mode, select **Enable**. (Deselecting the Admin Mode check box retains the session configuration but disables it.)

STEP 8 For the Destination Interface, select **Enable** and select a Destination Interface port to mirror the data.

CAUTION When a port is configured as a destination probe port, the switch does not forward or receive any traffic on that port and it does not respond to any pings received on that port. All the previous configuration parameters on that port are cleared and the port must be reconfigured when mirroring is removed from the port configuration.

Select Reset Session to clear any configuration parameters applied during this session.

STEP 9 Click **Apply** and then click **Close**. The probe session begins.

NOTE To end a probe session, select the session in the Port Mirroring Session Table and click **Edit**. Clear the Admin Mode checkbox, click **Apply**, and then click **Close**.

To clear the current configuration for a session, select the session and click **Edit**. Then select **Enable** for Reset Session field.

CPU/Memory Utilization

Use the *CPU/Memory Utilization* page to monitor CPU and memory usage. To display this page, click **Administration** > **Diagnostics** > *CPU/Memory Utilization* in the navigation window.

The page displays the following data:

- **Refresh Rate**—Specify that the page refresh with the latest data every 15, 30, or 60 seconds, or leave the default as No Refresh.
- **CPU Utilization Report**—The utilization percentage for 5 second, 1 minute, and 5 minute intervals.
- **Memory Utilization Report**—The following data is reported:
  - **Allocated Memory**—Amount of memory available to the operating system (OS).
  - **Free Memory**—Amount of memory available to the OS that is currently free.
  - **Total Memory**—Total system memory, which includes the Allocated Memory, plus free memory, plus memory reserved for use by code and data sections of the software image.

Enabling Bonjour

Bonjour enables the switch and the services enabled by the administrator to be discovered by using multicast DNS (mDNS). (Use the Administration > Management Services page to enable or disable the switch services.) Bonjour advertises switch services to the network and answers queries for the service types it supports, simplifying network configuration in small business environments.

Bonjour is enabled by default and runs on the management VLAN. Bonjour Discovery can only be enabled globally, not on a per-port or per- VLAN basis.

The switch advertises the following service types:

- **Cisco-specific device description** (csco-sb)—This service enables clients to discover Cisco switches and other products deployed in small business networks.
- **Management user interfaces**—This service identifies the management interface available on the switch (HTTP).

When a Bonjour-enabled switch is attached to a network, any Bonjour client can discover and get access to the management interface without prior configuration.

A system administrator can use an installed Internet Explorer plug-in to discover the switch. The web-based switch configuration utility shows up as a tab in the browser.

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. Bonjour works in both IPv4 and IPv6 networks.

To enable the switch to be discovered through Bonjour:

STEP 1 Click **Administration** > **Discovery - Bonjour** in the navigation window.

STEP 2 Select Enable.

STEP 3 Click **Apply**.

LLDP-MED

The IEEE 802.1AB standard, Link Layer Discovery Protocol (LLDP), describes a method by which stations residing on a LAN advertise identification information, capabilities, and physical descriptions. The information is exchanged in LLDP data units (LLDPDUs) which comprise type-length-value (TLV) structures. Various TLVs might be included in LLDPDUs, depending on the information that the administrator configures the port to advertise.

Information learned through LLDPDUs is stored in MIBs, and the information might be accessible by a network management system (NMS) such as SNMP. This framework is extensible and allows advanced utilization in areas such as VoIP networks.

NOTE LLDPDUs only communicate information; they do not automatically configure the switch.

The switch supports the LLDP Media Endpoint Discovery (LLDP-MED) extensions to the LLDP protocol. LLDP-MED enables auto-discovery of LAN policies, device location, and other device characteristics, and automates management of Power-over-Ethernet (PoE) endpoints.

See the following topics for more information on the configuration pages available in the Administration > Discovery - LLDP menu:

- **Configuring Global LLDP-MED Properties**
- **Configuring LLDP-MED on a Port**
- **LLDP-MED Port Status Details**
- **LLDP-MED Neighbor Information**

Configuring Global LLDP-MED Properties

Use the *LLDP MED Properties* page to specify global parameters for this feature.

To configure global LLDP-MED properties:

STEP 1 Click **Administration** > **Discovery - LLDP-MED** > **Properties** in the navigation window.

The LLDP-MED specification defines two primary device classes: Network Connectivity devices and Endpoint devices. As indicated in the Device Class field, the switch is classified as a Network Connectivity device.

STEP 2 For **Asset ID**, enter the asset ID for the switch, advertised in Inventory TLVs.

STEP 3 Specify the Location Parameters to identify the physical location of the switch:

- **Subtype**—Select one of the following options to configure how the switch location is identified in TLVs:
  - **Coordinate Based**—Switch location is identified using GPS coordinates in hexadecimal format.
  - **Civic Address**—Switch location is identified using a geographic description of the location, such as city, street name, and building name.
  - **ELIN**—Switch location is identified using the Emergency Location Identification Number (ELIN) of the switch.

- **Coordinates**—Switch GPS coordinates in hexadecimal format.
- **ELIN Address**—The ELIN number.
- **Country**—Country where the city is located. This is a two-character code as defined by ISO 3166.
- **City**—City where the street is located.
- **Street**—Street where the building is located.
- **Building**—Building in which the switch is located.

NOTE: The City, Street, and Building fields share the maximum character limitation; i.e., an entry in one field reduces the maximum allowable characters in the others. The maximum combine length of the city, street, and building fields is 246 characters. The characters ', ", %, and ? are not supported.

STEP 4 Click **Apply**. Your changes are saved to the Running Configuration.

Configuring LLDP-MED on a Port

The LLDP for Media Endpoint Devices (LLDP-MED) protocol provides extensions to the LLDP standard for network configuration and policy, device location, Power-over-Ethernet management, and inventory management.

Use the *LLDP-MED Port Settings* page to view and configure LLDP-MED operation on ports.

To configure these settings on a port:

STEP 1 Click **Administration** > **Discovery - LLDP-MED** > **LLDP-MED Port Settings** in the navigation window.

Each entry in the LLDP-MED Port Settings Table displays the LLDP-MED configuration for a port.

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

STEP 3 Specify the following for the selected port:

- **LLDP-MED Status**—Select to enable LLDP-MED operation on the port.
- **Configuration Notification**—Select to enable the switch to send notifications when there are topology changes on the network.

STEP 4 Select the Available TLVs that you want the port to include in LLDP advertisements:

- **Network Policy**—VLAN ID, the 802.1p class-of-service value, and the Differentiated Services Code Point (DSCP) value. This information is used to implement the Voice VLAN feature (see **Voice and Media**).
- **Location**—This value could include the hexadecimal GPS location coordinates for the switch, the civic address, or the ELIN address depending upon what is configured in **Configuring Global LLDP-MED Properties**.
- **PSE**—Indicates whether the port advertises itself as Power Sourcing Equipment capable of providing power to a connected Power-over Ethernet device. This option appears only on switches that include the PoE features.
- **Inventory**—Hardware and software version information.
- **System Capabilities**—Identifies the basic functionality of the switch such as bridging.

  NOTE The Application Type is included in the Network Policy TLV. Application types include Voice, Voice Signaling, Guest Voice, Guest Voice Signaling, Softphone Voice, Video Conferencing, Streaming Video, and Video Signaling. These Network Policies can be added to interfaces by using the **VLAN Management** > **Voice and Media** > **Media VLAN** page.

STEP 5 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

NOTE You can click **Configure Network Policy** to display the *Media VLAN* page. (You can also click **VLAN Management > Voice and Media > Media VLAN** in the navigation window.) This page enables you to assign LLDP-MED applications to VLANs and configure priority settings for associated traffic.

LLDP-MED Port Status Details

The *LLDP-MED Port Status Details* page displays the LLDP-MED configuration for all ports on which the feature is enabled. To display this page, click **Administration** > **Discovery - LLDP-MED** > **LLDP-MED Port Status Details** in the navigation window.

Select a port from the Port list. The Network Policies Table shows the fields for each service or policy advertised through LLDP:

- **Media Policy Application Type**—Type of service, such as Voice, associated with the LLDP network policy.
- **VLAN ID**—VLAN ID associated with the network policy.
- **Priority**—802.1p class-of-service value associated with the network policy.
- **DSCP**—DSCP value for the network policy.
- **Tagged**—Network policy is defined for tagged VLANs.

The following switch parameters are advertised in Inventory TLVs.

- **Hardware Revision**—Switch hardware revision ID.
- **Firmware Revision**—Switch firmware revision number.
- **Software Revision**—Switch software revision number.
- **Serial Number**—Switch serial number.
- **Manufacturer Name**—Switch manufacturer name.
- **Model Name**—Switch model name.
- **Asset ID**—LLDP-MED asset ID for the switch.

The following switch parameters are advertised in System TLVs.

- **Chassis ID**—The hardware address of the switch.
- **Chassis ID Subtype**—The type of hardware address.
- **System Description**—A preconfigured system description.
- **System Name**—The user-configured hostname (see the *System Settings* page).
- **Management Address SubType**—The protocol version for the management IP address.

- **Management Address**—The management interface IP address (see the *IPv4 Interface* page or the *IPv6 Interface* page).
- **Port ID SubType**—The type of the port identifier.
- **Port ID**—The port identifier.
- **Port Description**—The port description.
- **System Capabilities Enabled**—The capabilities that are enabled on the switch.
- **System Capabilities Supported**—The capabilities that are currently advertised as supported by the switch.

The following switch parameters are advertised in Location TLVs.

- **Subtype**—The supported type of location information (civic, ELIN, or coordinate-based).
- **Coordinates**—Switch GPS coordinates in hexadecimal format, if coordinate-based location information type is used.
- **ELIN Address**—The ELIN number, if this location information type is used.
- **Country**—Country where the city is located, if the civic location information type is used.
- **City**—City where the street is located, if the civic location information type is used.
- **Street**—Street where the building is located, if the civic location information type is used.
- **Building**—Building in which the switch is located, if the civic location information type is used.

LLDP-MED Neighbor Information

The *Neighbor Information* page displays information received from other LLDP-MED-capable devices in the network. To display this page, click **Administration** > **Discovery - LLDP-MED** > **Neighbor Information** in the navigation window.

The Neighbor Information Table displays the following fields for each LLDP neighbor device for which an advertisement has been received:

- **Local Port**—Port number of the switch where the LLDP advertisement was received.
- **Remote ID**—An internal identifier to uniquely identify each Neighbor.
- **Remote Port ID**—Name of the port through which the neighbor device sent the advertisement.
- **Device Class**—Advertised class of the remote device.

You can select an entry and click **Details** to display additional information from the LLDP-MED advertisement from the neighbor.

The *Neighbor Information—Details* page displays the following information:

MED Capabilities

- **Capabilities Supported**—Advertised capabilities of the device.
- **Capabilities Enabled**—Advertised capabilities that are enabled on the device.
- **Device Class**—Advertised class of the remote device.

Network Policies

- **Media Policy Application Type**—Type of service, such as voice, associated with the LLDP network policy.
- **VLAN ID**—VLAN ID associated with the network policy.
- **Priority**—802.1p class-of-service value associated with the network policy.
- **DSCP**—DSCP value for the network policy.
- **Unknown**—Neither the 802.1p value nor the DSCP value is configured for this Network Policy.
- **Tagged**—network policy is defined for tagged VLANs.

Inventory

- **Hardware Revision**—Switch hardware revision ID.
- **Firmware Revision**—Switch firmware revision number.
- **Software Revision**—Switch software revision number.
- **Manufacturer Name**—Switch manufacturer name.
- **Model Name**—Switch model name.
- **Asset ID**—LLDP-MED asset ID for the switch.

Location

- **Subtype**—Select one of the following options to configure how the switch location is identified in TLVs:
  - **Coordinate Based**—Switch location is identified by using GPS coordinates in hexadecimal format.
  - **Civic Address**—Switch location is identified by using a geographic description of the location, such as city, street name, and building name.
  - **ELIN**—Switch location is identified by using the Emergency Location Identification Number of the switch.
- **Location Information**—Switch location information, in the format specified by the Subtype field.

Extended PoE

- **PoE Device Type**—If PoE functionality is advertised, this field indicates whether the device is a Powered Device (PD) or Power Sourcing Equipment (PSE).

Extended PoE PD

If the device is powered by PoE, the following properties can be advertised:

- **PoE Power Value**—Power in watts requested by the device.
- **PoE Power Source**—Indicates how the powered device receives power:
  - **Primary**—A power supply is connected directly to the device.
  - **Backup**—The device receives power from a PoE power sourcing equipment.

- **PoE Power Priority**—Displays High, Low, or Critical to indicate how the port is prioritized when there is less PoE power to deliver than requested by all powered devices.

Configuring DHCP Client Vendor Options

You can configure the DHCP client functionality on the switch to include vendor information in its DHCP requests (DHCP option 60). A DHCP server might use vendor information to differentiate between clients based on the identified hardware type or functionality.

To configure DHCP vendor option string:

STEP 1 Click **Administration** > **DHCP Options** in the navigation window.

In addition to the vendor option and string, the page displays the format that the switch uses when obtaining its timezone information from a DHCP server. To configure the switch to acquire its timezone from DHCP, see **Time Settings**. If timezone information has been received, it displays the information. The Timezone Info Received field displays the information received, or displays False if no information has been received.

STEP 2 Select Enable for the Vendor Option.

STEP 3 Enter a value in the Vendor Option String text box.

STEP 4 Click **Apply**. Your changes are saved to the Running Configuration.

4

Port Management

This chapter describes how to configure switch port settings, combine ports into link aggregation groups, and configure port power features.

The following topics are included:

- **Configuring Port Settings**
- **Link Aggregation**
- **Configuring PoE**
- **Green Ethernet**

Configuring Port Settings

The *Port Settings* page enables you to administratively enable and disable ports and to configure autonegotiation of port speed and duplex mode. You can also use this page to configure flow control on the port.

To configure port settings:

STEP 1 Click **Port Management** > **Port Settings** in the navigation window.

STEP 2 Select the interface to configure, and then click **Edit**.

STEP 3 Specify the following for the selected port:

- **Administrative Status**—Select Up to enable the port or Down to disable it.
- **Auto Negotiation**—Select Enable to allow the switch autonegotiate the port speed and duplex mode with the connected device. If Autonegotiation is enabled, the Administrative Port Speed and Duplex Mode fields are not editable.
- **Administrative Port Speed**—If Auto Negotiation is disabled, select whether the port is capable of 10 Mbit/s or 100 Mbit/s operation.

- **Administrative Duplex Mode**—If Auto Negotiation is disabled, select Half for half-duplex or Full for full-duplex operation.
- **Admin Advertisement**—If Autonegotiation is enabled, select the highest port speed and duplex setting that you want the port to negotiate. If you select Max Capacity, the port autonegotiates up to the highest port speed and duplex setting supported by hardware.
- **Flow Control**—Select to enable IEEE 802.3x flow control. Flow control reduces data loss when the port cannot keep up with the number of frames being switched. When enabled, the switch can send a PAUSE frame to stop traffic on a port if the amount of memory used by packets on the port exceeds a preconfigured threshold. The paused port does not forward packets for the period of time specified in the PAUSE frame. When the PAUSE frame time elapses or memory utilization falls below a specified low threshold, the switch enables the port to again transmit frames. When the mode is set to half–duplex, back pressure is exerted; however, we recommend that **Flow Control** be enabled.
- **Member in LAG**—Indicates whether the port is a member of a Link Aggregation Group. See **Link Aggregation** for information on configuring LAGs.
- **MTU**—Specify the maximum transmission unit size in bytes. The default MTU is 1518 and the range is between 1518 and bytes.

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Link Aggregation

Link Aggregation allows one or more full-duplex Ethernet links to be aggregated together to form a Link Aggregation Group (LAG). The switch treats the LAG as if it is a single physical port, with improved fault tolerance and load- sharing capability.

A LAG interface can be either static or dynamic:

- **Static LAG**—Ports are assigned to a LAG directly by the administrator. The ports remain dedicated LAG members until configured otherwise.
- **Dynamic LAG**—A dynamic LAG is configured with one or more candidate ports. The LAG is formed by exchanging Link Aggregation Control Protocol Data Units with the remote device connecting to the candidate ports. When formed, the LAG might include only a subset of the eligible ports, depending on the port number limitations for LAGs and other factors. Candidate ports that are not selected as active member ports of a LAG are standby ports. A standby port may be selected as an active member when an active port in the same LAG fails.

The following topics provide additional information on the configuration pages available in the Port Management > Link Aggregation menu:

- **Configuring LAGs**
- **Configuring LAG Settings**
- **Configuring LACP**

Configuring LAGs

The switch supports up to 4 LAGs, with 8 ports per LAG. Use the *LAG Management* page to assign ports to LAGs and LACPs.

To display this page, click **Port Management** > **Link Aggregation** > **LAG Management** in the navigation window.

Four dynamic LAGs are preconfigured by default named *ch1* through *ch4*. They have no port members and are disabled.

You can add or remove ports to or from a LAG without disrupting traffic on the LAG.

LAGs can be assigned membership in VLANs; however, individual ports lose their individual VLAN memberships when they become LAG members. When a port is removed from a LAG, it rejoins the VLANs that it previously belong to as specified in the startup configuration.

To configure a LAG:

STEP 1 Select a LAG to configure, and then click **Edit**.

STEP 2 Specify the following for the selected LAG:

- **LAG Name**—Enter up to 15 alphanumeric characters to identify the LAG.
- **Type**—Select Static to manually assign ports to the LAG. Select Dynamic to enable the ports to exchange LACPDUs to dynamically form the LAG.
- **Port List/LAG Member**—To add or remove ports from a static LAG, select each port and click the left or right arrow to move it between the Port and LAG Member lists.

STEP 3 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Configuring LAG Settings

You can use the *LAG Settings* page to administratively enable or disable a LAG and configure load balancing settings.

To configure LAG settings:

STEP 1 Click **Port Management** > **Link Aggregation** > **LAG Settings** in the navigation window.

The LAG Settings Table lists each available LAG.

STEP 2 Select a LAG to configure, and then click **Edit**.

STEP 3 Specify the following for the selected LAG:

- **Administrative Status**—Select Up or Down to administratively enable or disable the LAG. When a LAG is disabled, its member ports operate as standalone physical ports.

- **Load Balance Algorithm**—Select one of the options to enable the switch to load-balance outgoing packets among member ports of a LAG. The switch selects one of the links in the channel for transmitting specific packets. The switch prioritizes each criteria for load balancing in the order listed in the option. The options are:
  - **Src/Dest MAC, VLAN, EType, incoming port**—Source and destination MAC addresses, the VLAN membership, the Ethertype field, and the port on which the packet was received.
  - **Src/Dest IP and TCP/UDP Port Fields**—Source and destination IP address and the TCP or UDP port number in the IP packet.

  If the IP packet option is selected, non-IP packets received on the port are balanced using the Src and Dest MAC address.
- **MTU**—Specify the maximum transmission unit size in bytes. The default MTU is 1518 and the range is between 1518 and bytes.

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Configuring LACP

The switch uses the Link Aggregation Control Protocol (LACP) to automate the formation of dynamic LAGs. LACP-enabled ports send protocol data units (LACPDUs) to detect each other on a network and negotiate a LAG.

Use the *LACP* page to view and configure protocol operation.

To configure LACP settings on individual ports:

STEP 1 Click **Port Management** > **Link Aggregation** > **LACP** in the navigation window.

The LACP Interface Table displays the following information for each port:

- **LACP Mode**—The administrative status of LACP mode (Enabled or Disabled)

The table displays the following information for the port when the port is the Actor (local) port:

- **System Priority**—A nonconfigurable system priority assigned to the switch.

- **Admin Key**—A number that determines the dynamic LAG(s) that the interface can join. All interfaces in a dynamic LAG must share the same admin key.
- **Port Priority**—A nonconfigurable priority assigned to the port.
- **LACP Aggregation**—The port mode with respect to link aggregation. This field is not configurable. Possible values are:
  - **Aggregate**—The port is participating in link aggregation.
  - **Individual**—The port is not participating in link aggregation and is functioning as an individual standalone port.
- **LACP Passive**—This field is always set to Active for all ports and is not configurable. It indicates that the port will continue to transmit LACPDUs after the LACPDU timeout has elapsed, regardless of the status of the link partner.
- **LACP Timeout**—The time after which an LACPDU is no longer valid (Long or Short).

The Table also displays the LACP Aggregation, LACP Passive, and LACP timeout values for the port when the port is the Partner (remote) port.

To edit the LACP settings:

STEP 1 Select the port to configure and click **Edit**.

STEP 2 Configure the following settings for the selected port:

- **Mode**—Check the box to enable LACP on the port.
- **Actor Timeout**—Information from the actor is no longer valid after the timeout period elapses.
  - **Short**—Short LACP timeout is 3 times the short periodic timer to transmit LACP packets. The default Short LACP timeout is 3 seconds.
  - **Long**—Long LACP timeout is 3 times the long periodic timer to transmit LACP packets. The default Long LACP timeout is 90 seconds.
- **Partner Timeout**—Information from the partner is no longer valid after the timeout period elapses.
  - **Short**—Short LACP timeout is 3 times the short periodic timer to transmit LACP packets. The default Short LACP timeout is 3 seconds.

- **Long**—Long LACP timeout is 3 times the long periodic timer to transmit LACP packets. The default Long LACP timeout is 90 seconds.

STEP 3 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Configuring PoE

On the SF200E-24P switch, ports 1–6 and 13–18 can operate as Power-over-Ethernet (PoE) power-sourcing equipment (PSE). PSE ports can provide power to connected PoE Powered Devices (PD).

On switches with PSE ports, the following topics provide information on the configuration pages available in the Port Management > PoE menu:

- **Configuring PoE Properties**
- **Configuring PoE Port Settings**

NOTE These configuration pages do not display on switches that do not support PSE functionality.

Configuring PoE Properties

You can use the *Properties* page to configure whether the switch generates trap messages under certain conditions and to view current power settings.

To configure PoE properties:

STEP 1 Click **Port Management** > **PoE** > **Properties** in the navigating window.

STEP 2 Set the following parameters:

- **Power Trap Threshold**—Specify a percentage of total available system power. When the requested power on PoE ports exceeds the threshold, a trap is generated to the log.

- **Power Management Mode**—Select how the switch prioritizes the power that it provides to multiple ports:
  - **Static with Port Priority**—Static with priority power management. This algorithm pre-allocates power based on the configured power limit and the priority of the port.
  - **Dynamic with Port Priority**—Dynamic with priority power management. This algorithm supplies power to devices as long as the consumption is within the configured limit and priority. There is no pre-allocation of power.

  In both modes, a port with a higher port priority is given preference when the switch supplies power to multiple ports. If two or more port priorities are equal, the port with the lower port number is given preference.
- **Reset Mode**—Select Enable to enable the switch initialize all PoE ports state machines.

STEP 3 Click **Apply**. Your changes are saved to the Running Configuration.

NOTE This page displays the following data for PoE power on the switch:

- **Power:** The current power status. If *On*, the switch is currently providing power through PoE to a connected device. If *Off*, the switch is not providing power through PoE to any connected devices.
- **Maximum Available Power**—The total power in watts that the switch is capable of making available to all PoE-capable ports.
- **Threshold Power**—The cutoff power value above which no additional PDs are powered. This threshold is calculated based on the Power Trap Threshold setting.
- **Allocated Power**—The total power in watts that the switch is actually providing to PoE ports.

Configuring PoE Port Settings

You can use the *Port Settings* page to view and configure settings for ports acting as PSEs.

To configure PoE settings for a port:

STEP 1 Click **Port Management** > **PoE** > **Port Settings** in the navigation window.

The PoE Setting Table displays which ports are enabled for PoE operation, their priority, power allocation in milliwatts, and other settings for each port.

STEP 2 Select the port to configure and click **Edit**.

STEP 3 Configure the following settings:

- **PoE**—Check the Enable box to configure the port as a PSE.
- **Power Priority Level**—Select Critical, High, or Low to configure the port priority level, for the delivery of power to an attached device.

  The switch might not be able to supply power to all connected devices that request it. The port priority determines which ports supply power when adequate power capacity is not available for all enabled ports. For ports that have the same priority level, the lower-numbered port has higher priority. For a system delivering peak power to a certain number of devices, if a new device is attached on a high-priority port, power is shut down to a device on a low-priority port, and the new device is powered up.
- **Power Limit Type**— Select one of the following methods to limit the power that the switch provides to a connected device.
  - **Dot3AF**—The maximum power that can be delivered by the port is limited by the detected IEEE 802.3af class.
  - **User-defined**—The maximum power that can be delivered by the port is specified by the user. If you select this option, specify a value in the Power Allocation field.
  - **LLDP-MED**—The maximum power that can be delivered by the port is limited by the value in LLDP-MED TLVs received from a port device. The value specified by the device should be in the range of 3-16.2 watts. If it is not in this range, then the default value of 16.2 watts is used.

    Note: If the selected Power Limit Type is LLDP-MED, then the priority setting from the remote device is not honored; instead the switch uses the Power Priority Level setting configured for the port.

  - **Dot3AF and LLDP-MED**—The maximum power that can be delivered by the port is limited by the value in LLDP-MED TLVs received from a port device. The value specified by the device should be in the range of 3-16.2 watts. If it is not in this range, then the maximum power is limited by the IEEE 802.3AF class.
  - **User-Defined and LLDP-MED**—The maximum power that can be delivered by the port is limited by the value in LLDP-MED TLVs received from a port device. The value specified by the device should be in the range of 3-16.2 watts. If it is not in this range, then the maximum power is limited by the value that you specify in the Power Allocation field.

- **Power Allocation**—If you configured a user-defined option for Power Limit Type, enter the power in milliwatts to be allocated to the port, between 3000 to 16200 milliwatts.
- **Detection Type**—Select one of the following methods to detect PoE-powered devices connected to the ports.
  - **802.3af 4point** —Resistive signature devices detected with the first algorithm that correspond to the updated IEEE 802.3at-2009 PoE standard (also known as PoE+). It provides up to 51 W of power over a single cable by utilizing all four pairs in the Cat5 cable.
  - **802.3af 2point**—Resistive signature devices detected with the first algorithm that correspond to the original IEEE 802.3af-2003 PoE standard that provides up to 15.4 W of DC power (minimum 44 V DC and 350 mA) to each device.
- **Reset Mode**—Select Enable to enable the switch initialize the ports PoE state machines.

The following statistics also appear:

- **Power Consumption**—Actual power consumption on the port.
- **Overload Counter**—Total number of power overload occurrences.
- **Short Counter**—Total number of power short condition (electrical shorts) on a port.
- **Denied Counter**—Number of times the powered device was denied power.
- **Absent Counter**—Number of times the power supply was stopped to the powered device because the powered device was no longer detected.

- **Invalid Signature Counter**—Number of times an invalid signature was received. Signatures are the means by which the powered device identifies itself to the PSE. A signature is generated during powered device detection, classification, or maintenance.

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Green Ethernet

The switch provides a Green Ethernet power saving feature on gigabit Ethernet copper ports called Energy Detect Mode. This feature helps reduce chip power by forcing a port PHY into a low-power mode when the signal from a copper link partner is not present. (PHY is an abbreviation for the physical layer of the OSI model.)

When the Energy Detect is enabled, the switch automatically enters the low-power mode when energy on the line is lost, and it resumes normal operation when energy is detected. When the port PHY is in low-power mode, the PHY wakes up after a certain period of time, and sends link pulses to monitor for energy from the link partner. If energy is detected while the port is in wake-up mode, the switch returns the port to normal operation. When the wake-up period expires, the port returns to low-power mode.

Energy Detect works whether the port has autonegotiation enabled or disabled, and can be enabled or disabled by the administrator. The Energy Detect Mode properties are configurable per-port.

See the following topics for more information on the configuration pages available in the Port Management > Green Ethernet menu:

- **Configuring Green Ethernet Properties**
- **Configuring Green Ethernet Port Settings**

Configuring Green Ethernet Properties

You can use the *Green Ethernet Properties* page to enable Green Ethernet functionality globally. The global settings are applied to all ports.

NOTE You can override the global settings by configuring these features on individual ports (see **Configuring Green Ethernet Port Settings**); however, changes you subsequently make to the global settings override any custom port configuration.

To configure global Green Ethernet properties:

STEP 1 Click **Port Management > Green Ethernet > Properties** in the navigation window.

By default, Energy Detect mode is enabled globally and on all ports.

STEP 2 If not already enabled, select Energy Detect Mode to enable this feature on the switch. The switch automatically enters the low-power mode when energy on the line is lost, and it resumes normal operation when energy is detected.

STEP 3 Click **Apply**. Your changes are saved to the Running Configuration.

Configuring Green Ethernet Port Settings

Use the *Green Ethernet Port Settings* page to view and configure Energy Detect settings on individual ports.

NOTE Energy Detect port settings are overridden if the global settings are subsequently changed (see **Configuring Green Ethernet Properties**).

To configure Green Ethernet port settings:

STEP 1 Click **Port Management > Green Ethernet > Port Settings** in the navigation window.

The Settings page displays the following Energy Detect fields for each port:

- Admin—Indicates whether Energy Detect is enabled on the port.
- Operational—Indicates whether Energy Detect mode is currently operational ("Enabled") on the port.
- Reason—Indicates why the operational status is enabled or disabled.

  The following reason may display when the Energy Detect operational status is Enabled.

  - *No Energy Detected*—No energy is detected on the link.

  The following reasons might display when the Energy Detect operational status is Disabled.

  - *Fiber*—The administrative status might be active but the port is functioning in fiber mode. (Green Ethernet functionality applies only to copper ports.)

- *Link up*—There is activity on the link.
- *Admin Down*—Energy detect mode is administratively disabled.

STEP 2 Select the port to configure and click **Edit**.

STEP 3 Select Energy Detect to administratively enable Energy Detect on the port.

STEP 4 Click **Apply** to save any changes to the Running Configuration.

5

VLAN Management

This chapter describes how to configure virtual LANs.

It includes the following topics:

- **Creating VLANs**
- **Configuring VLAN Interface Settings**
- **Configuring VLAN Membership**
- **Configuring Port VLAN Membership**
- **Setting the Default VLAN**
- **Voice and Media**

Virtual LAN (VLAN) on a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast. Like a router, it partitions the network into logical segments, providing better administration, security, and management of multicast traffic.

A VLAN is a set of end stations and the switch ports that connect them. You might have many reasons for the logical division, such as department or project membership. The only requirement is that the end station and the port to which it is connected both belong to the same VLAN(s).

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag, also known as VLAN tag, in the Layer 2 header of packets transmitted on a VLAN. If an end station omits the tag, or the VLAN portion of the tag, the first switch port to receive the packet either rejects it or inserts a tag matching its default VLAN ID. A port can handle traffic for more than one VLAN, but it can only support the Port VLAN ID (PVID).

The switch is pre-configured with VLAN ID 1 as the Default VLAN. All ports are members of this VLAN, and use its VLAN ID (1) as their PVID.

Creating VLANs

The *Create VLAN* page enables you to define and configure VLANs on the network. To display this page **VLAN Management** > **Create VLAN** in the navigation window.

The VLAN Table displays the VLAN ID, name, if one exists, and type for the pre-configured VLAN (VLAN ID 1) and any VLANs that you add. One port must be configured as the Default VLAN. The type for all other VLANs is Static. The switch is pre-configured with VLAN ID 1 as the Default VLAN. All ports are members of this VLAN, and use its VLAN ID (1) as their PVID.

If you create additional VLANs, you can configure one of them as the Default VLAN. (See **Setting the Default VLAN**.) The configured Default VLAN cannot be deleted. A Static VLAN can be deleted. However, VLAN ID 1 cannot be deleted, even if it is configured as a Static VLAN.

You can create up to VLANs, and assign VLAN IDs up to 4094. To create a new VLAN or a range of VLANs:

STEP 1 Click **Add**.

STEP 2 Select VLAN and enter a VLAN ID.

Or, create a range of VLANs by selecting Range and specifying the beginning and ending VLAN IDs in the range.

STEP 3 If you are creating a single VLAN, you can enter an optional VLAN name for easy reference.

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Configuring VLAN Interface Settings

You can use the *Interface Settings* page to view and configure port VLAN tagging capabilities. To display this page click **VLAN Management** > **Interface Settings** in the navigation window.

The Interface Setting Table shows the VLAN configuration for each port. To display the VLAN configuration on link aggregation groups, select LAG from the Interface Type list.

To configure VLAN interface settings:

STEP 1 Select the port or LAG to configure and click **Edit**.

STEP 2 Configure the following settings for the selected port or LAG:

- **Interface VLAN Mode**—Select an option to configure the port type with respect to VLAN membership and tagging.
  - **General**—The port can be a member of one or more tagged or untagged VLANs. This mode allows the full capabilities specified in the IEEE 802.1Q specification, "VLAN Tagging."
  - **Access**—The port can accept only untagged frames. An access port can be a member of only one VLAN and it uses the VLAN ID as its port VLAN ID (PVID). Access ports are typically used to connect hosts, which become members of the VLAN by virtue of being physically connected to the port.
  - **Trunk**—The port can be assigned to only one untagged VLAN, the *native VLAN,* and can be assigned to any number of tagged VLANs (or none). Trunk ports carry traffic for multiple VLANs from the switch to other network devices, such as an upstream router or an edge switch.
- **PVID**—(General ports only) The port VLAN ID indicates the default VLAN that the interface is a member of. Set the PVID equal to a VLAN ID where the port is an untagged member. (For Access ports, the PVID is automatically set to the Access VLAN ID. For Trunk ports, the PVID is set to the configured Native VLAN ID or, if None is configured, to the default VLAN ID.)
- **Native VLAN**—(Trunk ports only) The native VLAN identifies the one untagged VLAN membership for a trunk port. Select one of the following:
  - **None**—The port has no untagged VLAN membership. The PVID for the port is set to the default VLAN ID.
  - **Default**—The Native VLAN equals the default VLAN. The PVID for the port is also set to the default VLAN ID.
  - **User defined**—The VLAN ID you specify is used as the untagged VLAN membership for the Trunk port. The PVID for the port is also set to the specified VLAN ID.
- **Access VLAN**—(Access ports only) An access port can be a member of only one VLAN, the Access VLAN. The port VLAN ID is set to the Access VLAN ID.

- **Frame Type**—Specifies the frame type accepted on the port:
  - **Admit Untagged Only**—Only untagged frames are accepted on the port. Tagged frames are discarded.
  - **Admit Tagged Only**—Only tagged frames are accepted on the port. Untagged frames are discarded.
  - **Admit All**—Both tagged and untagged frames are accepted on the port.

  An access port can admit untagged frames only. A trunk port can be assigned to only one untagged VLAN, called the *native VLAN* and, can be assigned to any number of tagged VLANs (or none). If a trunk port is member of both untagged and tagged VLANs, it admits all frame types. If the trunk port is member of tagged VLANs only, it admits tagged frames only.
- **Ingress Filtering**—Select to enable ingress filtering on the port. When ingress filtering is enabled, the switch accepts frames only from the VLANs of which it is a member. It discards frames received from other VLANs. All ports in access or trunk mode will always have their Ingress Filtering enabled. Disabling and enabling Ingress Filtering is only available on ports set to General Mode.
- **VLAN Priority**—The default 802.1p priority value for the port. The value will be applied to the incoming packets based on the QoS trust mode configured at the port and the types of the packets. See **QoS Properties** for information and instructions on configuring the port trust mode.

STEP 3 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Changing the Interface VLAN Mode

When the interface VLAN mode of a port is changed, the switch automatically handles the affected VLAN membership configuration, as follows:

Changing from Access Port to Trunk Port

The VLAN configuration remains unchanged. The Access port VLAN becomes the native VLAN for the Trunk port. The port must follow the restrictions for Trunk ports.

Changing from Trunk Port to Access Port

If the original trunk port has an untagged VLAN member on the port, the port is removed from all its VLANs except the untagged VLAN on the port. The PVID is set to the untagged VLAN ID.

If the original Trunk port does not have an untagged VLAN member on the port, the port is removed from all its VLANs and becomes a member of the default VLAN. Its PVID is set to the default VLAN ID and the port is set to admit only untagged or priority-tagged packets. The port is untagged for the default VLAN.

Changing from Access Port to General Port

The VLAN configuration remains unchanged except that the port can now admit all frames. As a General port, it can be a tagged or an untagged member of any VLAN.

Changing from General Port to Access Port

If the General port has no untagged VLAN membership that provides the PVID for the port, when the port is changed to an Access port it is removed from all the General port's VLANs and becomes an untagged member of the default VLAN. The Access port PVID is set to the default VLAN.

The Access port admits only untagged or priority-tagged packets.

Changing from Trunk Port to General Port

The VLAN configuration remains unchanged. As a General port, the port can be a tagged or an untagged member of any VLAN.

Changing from General Port to Trunk Port

The VLAN configuration remains unchanged. The PVID of the General port is used to configure the native VLAN of the Trunk port. The port must follow the restrictions of the Trunk port.

For example, assume a General port is an untagged member of VLANs 1, 10, and 20, and the port's PVID is 1.

When the port is changed to a Trunk port, VLAN 1 becomes the native VLAN. The Trunk port remains a member of VLANs 10 and 20, but now with tagging enabled.

Deleting a VLAN

When a VLAN is deleted, the following actions occur:

- If the deleted VLAN was a Trunk port's native VLAN, the trunk port's native VLAN and PVID are changed to the default VLAN.

- If an Access port was a member of the deleted VLAN, the Access port becomes a member of the default VLAN and its PVID is changed to the default VLAN.
- If a General port was configured to use the VLAN ID as its PVID, the General port's PVID is changed to the default VLAN ID. No other VLAN memberships are changed.

Configuring VLAN Membership

You can use these pages to view and configure VLAN memberships:

- The *Port to VLAN* page enables you to select a VLAN and configure its member ports. See **Configuring Port to VLAN**.
- The *Port VLAN Membership* page enables you to select a port and configure it as a member of one or more VLANs. See **Configuring Port VLAN Membership**.

By default, all ports are members of VLAN 1. You can change the VLAN membership of any port. VLAN memberships can be configured as tagged or untagged.

- If the switch receives an untagged frame from a VLAN, the switch will insert a VLAN tag before forwarding the frame to the egress ports that are configured as tagged members of the VLAN.
- If the switch receives an untagged frame from a VLAN, the switch will forward the frame as is to egress ports that are configured as untagged members of the VLAN.
- If the switch receives a tagged frame from a VLAN, the switch will remove the VLAN tag before forwarding the frame to the egress ports that are configured as untagged members of the VLAN.
- If the switch receives a tagged frame from a VLAN, the switch will forward the frame as is to egress ports that are configured as tagged members of the VLAN.

Configuring Port to VLAN

Use the *Port to VLAN* page to:

- Configure ports as members of a selected VLAN.
- Specify that when a port receives packets from the selected VLAN, the packets are tagged with the VLAN ID upon forwarding.
- Specify that the selected VLAN ID serves as the port VLAN ID (i.e., the selected VLAN ID is added when the port forwards packets that it receives with no VLAN membership).

To configure port VLAN memberships:

STEP 1 Click **VLAN Management** > **Port To VLAN** in the navigation window.

The configured interface port mode (access, trunk, or general) of each port affects how the port can be assigned to VLANs. See **Configuring VLAN Interface Settings** for instructions on configuring the port mode setting.

STEP 2 Select the VLAN ID to configure and use the Interface Type list to display either ports or LAGs.

STEP 3 For each interface, configure the following parameters:

- **Member**—Check this box if a port is to be member of the VLAN. Uncheck this box if a port is not to be member of the VLAN. A port is not member of the VLAN by default.
- **Tagged**—Select Tagged if all the packets of the VLAN egress to the port are to be tagged. Otherwise, select Untagged. A trunk port is tagged by default. This option is only relevant if the port is a member of the VLAN.
- **Untagged**—Select Untagged if the packets from the VLAN egress to the port are to be untagged. Otherwise, select Tagged. An access port is always untagged. A general port is untagged by default. This option is relevant only if the port is a member of the VLAN.
- **PVID**—Check this box if a port is to use the selected VLAN ID as its port VLAN ID (PVID). Otherwise, uncheck this box. If PVID is selected for an access or trunk port, the port must be an untagged member of the VLAN. Untagged packets received from the port will be assigned to the corresponding VLAN.

STEP 4 Click **Apply**. Your changes are saved to the Running Configuration.

Configuring Port VLAN Membership

To configure VLAN settings for ports:

STEP 1 Click **VLAN Management** > **Port VLAN Membership** in the navigation window.

By default, the page displays VLAN information for each port. You can use the filter settings to display the VLAN information for LAG ports. The page displays the interface VLAN mode (Trunk, Access, or General), the PVID, and the VLAN membership(s). If a port is a member of multiple VLANs, you can select the port and click **Detail** to display this information for a single port.

STEP 2 Select a port or LAG to configure and click **Edit**.

STEP 3 To assign or remove a VLAN membership, use the arrow buttons as described below.

- To add a VLAN membership: Click a VLAN in the Available list, change its Tagging properties if needed (see below), and then click the right-arrow button to move it to the Selected list.
- To remove a VLAN membership: Click a VLAN in the Selected list, and then click the left-arrow button to move it to the Available list.

Tagging and PVID Properties

Depending on the interface VLAN mode (Trunk, Access, or General), when you select a VLAN in the Available list, you can specify the following properties for the interface before moving the VLAN to the Selected list for the interface.

- **Membership**—The interface can be configured as a tagged or untagged member of the selected VLAN.
  - **Tagged**—If selected, the port is a tagged member of the selected VLAN. When the switch forwards packets it receives for this VLAN through this interface, it adds the VLAN ID to the packet.
  - **Untagged**—If selected, the port will be an untagged member of the selected VLAN. When the switch forwards packets for this VLAN through this interface, it does not add the VLAN ID to the packet.

  If the interface VLAN mode is General, you can select either option for any VLAN. If the interface VLAN mode is Access, only one VLAN can be selected and the Untagged option must be selected for the interface. If the interface VLAN mode is Trunk, the interface can be specified as an Untagged member of one VLAN and can be specified as a Tagged member of other VLANs.

- **PVID**—When this option in selected, the port uses the selected VLAN ID as its port VLAN ID (PVID). The port assigns the PVID to all untagged frames received on the port before forwarding. The following configuration rules apply:
  - If the interface VLAN mode is General, any VLAN of which the interface is a Tagged or Untagged member can be selected to provide the PVID.
  - If the interface VLAN mode is Trunk, the PVID is set to the VLAN ID of which the port is a tagged member.
  - If the interface VLAN type is Access, the PVID is set to the Access VLAN ID and this field cannot be modified.

When you select the Untagged, Tagged, and PVID options and move the VLAN to the Selected list, a U, T, and/or P is appended to the VID.

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Setting the Default VLAN

By default, the switch automatically creates VLAN 1 as the default VLAN for all ports and link aggregation groups (LAGs). If a port has no VLAN memberships, the switch automatically configures it as a member of the default VLAN.

You can use the *Default VLAN Settings* page to change the default VLAN.

When the VID of the default VLAN is changed:

- Ports that were members of the original default VLAN are removed as members of that VLAN and are configured as members of the new default VLAN.
- The Port VLAN Identifier (PVID) of the ports that were members of the original default VLAN is changed to the VID of the new default VLAN.
- If the management VLAN was the same as the original default VLAN, then the management VLAN is updated to the new default VLAN provided there is at least one member port. If DHCP is enabled, the switch attempts to renew the switch IP address through DHCP.

- The type of the original default VLAN is changed from Default to Static, and it can be deleted. One exception is VLAN 1. Even if it is no longer designated as the default VLAN, VLAN 1 cannot be deleted.

To select a default VLAN:

STEP 1 Click **VLAN Management** > **Default VLAN Settings** in the navigation window.

STEP 2 Select the VLAN from the list.

STEP 3 Click **Apply**.

Voice and Media

Voice-over-Internet-Protocol (VoIP) allows using a computer data network for voice telephone calls. With the increased deployment of delay-sensitive applications such as VoIP in modern networks, proper QoS configuration is needed to ensure high-quality performance. The Voice and Media feature provides a simple classification mechanism for voice packets so that they can be prioritized above data packets.

The Voice and Media feature identifies VoIP streams in Ethernet switches and provides them with a better Class-of-Service (CoS) than ordinary traffic. The switch supports two types of Voice and Media:

- **Protocol-based**—Identifies a VoIP session using the Session Initiation Protocol (SIP) and H.323 control traffic, and assigns these packets the highest priority on the voice VLAN.
- **OUI-based**—Ports that are enabled for this feature automatically become members of the configured voice VLAN. The switch detects Organizationally Unique Identifier (OUI) values in the first three bytes of the MAC addresses in client packets to classify them on the VoIP VLAN and prioritize them on the Auto VoIP-enabled ports.

These topics for more information on the configuration pages available in **VLAN Management** > **Voice and Media**:

- **Displaying and Adding Telephony OUI**
- **Configuring OUI Based Voice and Media**
- **Configuring SIP/H323 Based Voice and Media**

- Media VLAN
- Auto VoIP Sessions

Displaying and Adding Telephony OUI

The *Telephony OUI* page lists the Organizationally Unique Identifiers (OUIs) associated with different voice VLANs.

To display this page, click **VLAN Management** > **Voice and Media** > **Telephony OUI** in the navigation window.

The Telephony OUI Table is preconfigured with identifiers for commonly used telephony devices. The administrator can add or remove OUIs. When Voice and Media is enabled, ports use the OUI digits in the source and/or destination MAC addresses of incoming packets to automatically assign voice traffic to a voice VLAN. See **Configuring OUI Based Voice and Media** for instructions on associating the VLAN with an IEEE 802.1p priority and enabling ports for Voice and Media.

To add a new OUI description:

STEP 1 Click **Add**.

STEP 2 Specify the following values:

- **Telephony OUI**—Enter a 3-octet identifier for the telephony application.
- **Description**—Enter a description of the service such as the vendor name or telephony product.

STEP 3 Click **Apply** and **Close**.

Configuring OUI Based Voice and Media

You can use the Telephony OUI Based Auto VoIP page to:

- Configure an IEEE 802.1p priority level for Voice and Media traffic identified using the OUI digits in MAC addresses.
- Specify the VLAN for OUI-based VoIP packets. Although you can assign a VLAN ID that has not yet been created on the switch, you must subsequently create the VLAN for the feature to be operational (see **Creating VLANs**).

- Enable ports for this feature. When enabled on a port, the port is automatically made member of the configured voice VLAN when the switch receives an OUI frame (the administrator does not need to manually add the port as a member of the VLAN).

The *Port VLAN Membership* page shows that the port is a member of the Voice VLAN.

To configure OUI-based Voice and Media:

STEP 1 Click **VLAN Management** > **Voice and Media** > **Telephony OUI Based** in the navigation window.

STEP 2 Check VLAN to enable modifying the VLAN ID and Priority fields.

STEP 3 In the VLAN ID field, specify the VLAN to carry voice traffic. This VLAN should already be configured on the switch (see **Creating VLANs**).

STEP 4 In the Priority field, specify the IEEE 802.1p Class-of-Service (CoS) priority level for VoIP traffic.

STEP 5 Click **Apply**. Your changes are saved to the Running Configuration.

STEP 6 In the Telephony OUI Based Interface Settings Table, select an interface to configure, and then click **Edit**.

NOTE: Set the an auto VoIP port to be a General port, not a Trunk or Access port.

STEP 7 Select Enable for the Auto VoIP mode. The port is automatically added as a member of the voice VLAN.

STEP 8 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Configuring SIP/H323 Based Voice and Media

You can use the *SIP/H323 Based Auto VoIP* page to configure the switch to recognize VoIP traffic by its protocol, such as the Session Initiation Protocol (SIP) and H.323. The traffic is automatically assigned the highest priority available on the system.

To configure SIP/H323 based Voice and Media:

STEP 1 Click **VLAN Management** > **Voice and Media** > **SIP/H323 Based** in the navigation window.

The table lists the administrative and operational statuses for SIP/H323 Auto VoIP on each interface, and shows the class that traffic will be assigned to. The traffic class corresponding to the highest priority queue on the port is chosen automatically.

STEP 2 Use the Interface Type menu to display ports or LAGs in the SIP/H323 Based Interface Settings Table.

STEP 3 Select the port or LAG interface to configure and click **Edit**.

STEP 4 Select Enable for the Auto VoIP Mode.

STEP 5 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Media VLAN

The Media VLAN feature enables switch ports to carry voice, video, and signaling traffic with an assigned priority value. Assigning different priorities to traffic enables separation of media and data traffic coming into a port. The Media VLAN feature helps to ensure that the sound or video quality of an IP phone or video device is safeguarded from deterioration when data traffic on the port is high.

The inherent traffic isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network-attached clients cannot initiate a direct attack on voice components. The switch uses the IP-DSCP or 802.1p value in packets from media devices to assign this traffic to high priority queues.

The switch uses Media VLANs to support LLDP-MED applications. (See **LLDP-MED** for information on the protocol.) Each Media VLAN corresponds to an LLDP-MED application for a specific type of media traffic. The LLDP-MED applications are voice, voice signaling, guest voice, guest voice signaling, softphone voice, video conferencing, streaming video, and video signaling. Each Media VLAN is associated with the following parameters

- A VLAN with optional VLAN tagging
- An IEEE 802.1p priority value
- A DSCP value

When a port is LLDP-MED enabled with network policy, the switch will advertise its Media VLANs in the LLDP-MED network policy TLVs out to the port. When a LLDP Media Endpoint is discovered, the switch will install the Media VLAN at the corresponding port. You can enable LLDP-MED and networking policy in the Administration > Discovery - LLDP pages.

Media VLAN is enabled and disabled globally. Each application and its Media VLAN is configured on a per-port basis. For example, Guest Voice can be on Media VLAN 1 on interface g1, but can be on Media VLAN 10 on interface g2.

The Media VLAN Interface Settings Table displays each media traffic type that can be enabled, and shows its status and settings on the selected port.

To configure Media VLAN applications:

STEP 1 Click **VLAN management > Voice and Media > Media VLAN** in the navigation window.

STEP 2 Select Enable for Admin Mode to globally enable this feature on the switch, and then click **Apply**.

STEP 3 Select an interface to configure from the Interface list.

CAUTION Ports that are members of a LAG cannot be enabled for Media VLAN applications (see **Configuring LAGs**).

STEP 4 From the Application list, select the media traffic type to configure:

- Voice
- Voice Signaling
- Guest Voice
- Guest Voice Signaling
- Softphone Voice
- Video Conferencing
- Streaming Video
- Video Signaling

STEP 5 Click **Edit**.

STEP 6 For Application Status, select Enable to enable priority assignment for the selected application. Uncheck the box to disable this feature.

STEP 7 If you enabled Application Status, enable or disable the following features:

- **Untagged**—Select Enable if the media device (LLDP-MED Endpoint) will send untagged packets. The network policy TLV from the switch must also indicate this expectation, and a media device must acknowledge that it will use untagged frames. Uncheck the box to disable this feature.
- **VLAN** and **VLAN ID**—Select Enable to specify a VLAN, and then choose a VLAN ID from the list. Uncheck the box to disable this feature.
- **Priority** and **Priority Value**—Select Enable to prioritize packets of the selected application. Then enter an IEEE 802.1p class-of-service priority tagging value for Media VLAN traffic. The priority tag range is 0–7.
- **DSCP** and **DSCP Value**—Select Enable to specify a DSCP for the selected application. Then enter a DSCP value for the port. The range is 0-63.

STEP 8 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

STEP 9 Ensure that LLDP-MED is enabled on the interface. You can click Enable LLDP-MED Network Policy to display the *LLDP-MED Port Settings* page. See **LLDP-MED** for more information.

Auto VoIP Sessions

The *Auto VoIP Sessions* page displays information about the source, destination, and protocol for each Voice over IP session.

6

Spanning Tree

This chapter describes how to configure the Spanning Tree Protocol (STP) on the switch.

It includes the following topics:

- **Overview of Spanning Tree**
- **Configuring STP Status and Global Settings**
- **Configuring STP Interface Settings**
- **RSTP Interface Settings**

Overview of Spanning Tree

STP enables efficient communication on a network that includes multiple bridges. Devices on these networks can learn multiple (that is, redundant) paths to the same endpoint. While path redundancy is desirable for maintaining traffic flow when particular links are down, it can lead to a traffic loops that affect network performance and confuse forwarding algorithms.

Each STP-enabled bridge exchanges Bridge Protocol Data Units (BPDUs) with other bridges. BPDUs identify the bridge port MAC addresses and the priority and cost associated with each port. STP uses this information to build a topology that provides one active path between any two stations on the network. Duplicate paths between those stations are placed in a stand-by state for use only when the active path becomes unavailable.

BPDU exchanges also facilitate the election of a root bridge and root port for the network. The root bridge provides a reference point that each other bridge uses to calculate a lowest-cost path by summing the cost of the ports in each path and choosing the one with the lowest total. The port that connects a bridge to the lowest-cost path is called the bridge's *root port*.

When the root bridge is selected and each root port is established, each network segment can then determine which bridge provides the lowest cost path to the root port. The port that provides this path is named the *designated port* for the network segment. Spanning tree disables other ports for that network segment or designates them as alternate or backup ports.

Supported spanning tree versions include Common Spanning Tree (CST) and Rapid STP (RSTP). This switch does not support Multiple STP (MSTP).

- CST (IEEE 802.1D) is the original protocol version that provides a single path between end stations, avoiding and eliminating loops.
- RSTP (IEEE 802.1D-2004 or IEEE 802.1w) provides protocol enhancements that enable a network to more quickly achieve an optimal STP topology. Spanning tree is enabled by default and set to be RSTP.

Configuring STP Status and Global Settings

You can use the *STP Status & Global Settings* page to enable STP, select the STP mode of operation, and configure bridge priority settings. You can also view status information about the STP topology. To display this page, click **Spanning Tree** > **STP Status & Global Settings** in the navigation window.

This page enables you to configure global settings and bridge settings, and displays information about the designated root.

Configuring Global and Bridge Settings

To configure STP global settings and bridge settings:

STEP 1 Specify the following global settings:

- **Spanning Tree State**—Select to enable STP operation on the switch. You must also enable STP operation on individual ports (see **Configuring STP Interface Settings**).

- **STP Operation Mode**—Select one of the following STP modes:
  - **Classic STP**—Operates according to the original IEEE 802.1D spanning tree protocol.
  - **Rapid STP**—Is the default value and provides faster spanning tree convergence after a topology change than does classic STP.
- **BPDU Handling**—Bridge Protocol Data Units (BPDUs) are the messages exchanged between switches to calculate STP topology. Select the method of BPDU packet handling when the spanning tree is disabled on an interface:
  - **Filtering**—Enables the port to discard BPDUs received on interfaces that are not enabled for STP.
  - **Flooding**—Allows flooding of BPDUs received on non-spanning-tree ports to all other non-spanning-tree ports.

STEP 2 Specify the following bridge setting:

- **Priority**—The bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest bridge identifier becomes the root bridge. The bridge priority must be a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest multiple of 4096. For example if you attempt to set the priority to any value between 0 and 4095, it will be set to 0. The default priority is 32768. The valid range is 0-61440.
- **CST Bridge Max Age**—The amount of time in seconds that a bridge waits before implementing a topological change. The valid range is 6-40 seconds. The default is 20 seconds.
- **CST Bridge Forward Delay**—The amount of time in seconds that a bridge remains in a listening and learning state before forwarding packets. The valid range is 4-30 seconds. The default is 15 seconds.

The following information appears in this section of the page:

- **Hello Time**—The interval at which a bridge sends configuration messages.
- **Max Hops**—The number of hops before a BDPU is discarded and the port information is aged out. The maximum hop count is set to 20 and is not configurable.
- **Hold Time**—The minimum time period, in seconds, that elapses between the transmission of Configuration BPDUs through a bridge port.

The following information appears in the Designated Root section of the page:

- **Bridge ID**—The bridge identifier, which is a concatenation of the bridge priority and the base MAC address of the bridge.
- **Root Bridge ID**—The Bridge ID of the root bridge. The bridge with the lowest Bridge ID among all the bridges become the root bridge.
- **Root Port**—The port number that offers the lowest-cost path from this bridge to the root bridge. It is significant when the bridge is not the root. The default is zero.
- **Root Path Cost**—The cost of the path from this bridge to the root.
- **Topology Changes Count**—The total amount of STP state changes that have occurred.
- **Last Topology Change**—The total amount of time since the last topographic change.

STEP 3 Click **Apply**. Your changes are saved to the Running Configuration.

Configuring STP Interface Settings

The *STP Interface Settings* page assigns STP properties to individual ports or LAGs. These settings are applicable to both the Classic STP and Rapid STP.

To edit settings for a port or LAG:

STEP 1 Click **Spanning Tree** > **STP Interface Settings** in the navigation window.

The STP Interface Settings Table displays configuration information for each port and LAG. By default, all ports are enabled for STP operation.

NOTE: The list ports/LAGs might span more than one page. Use the Page list to display the next set of entries.

STEP 2 Select the port or LAG to configure and click **Edit**.

STEP 3 Enter the parameters:

- **STP**—Select to enable STP operation on the port/LAG.
- **Auto Edge**—Select Enable to allow the switch to automatically determine if the port is an edge port or PortFast. A port is an edge port if it is not connected to a bridge. Auto-detection speeds up the transition of the port to forwarding state. A port can forward traffic and learn MAC addresses when it is in forwarding state.
- **Edge Port**—Select Enable to manually configure the port as an edge port.
- **BPDU Handling**—Bridge Protocol Data Units (BPDUs) are the messages exchanged between switches to calculate STP topology. Select the method of BPDU packet handling when the spanning tree is disabled on an interface:
  - **Filtering**—Enables the port to discard BPDUs received on interfaces that are not enabled for STP.
  - **Flooding**—Allows flooding of BPDUs received on non-spanning-tree ports to all other non-spanning-tree ports.
- **Path Cost**—Specify the port path cost. The cost of a path to the root bridge is the sum of the costs of all ports in the path. The path cost is used by CST and RSTP to forward traffic when a path is being rerouted. Select Use Default to set the path cost to the port speed. Or select User Defined to set a custom value between 0 and 200,000,000. A value of zero means the path cost is set according to the port's speed.

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

The new configuration appears in the STP Interface Settings Table along with the following information about the port/LAG.

- **Operational Edge Status**—Indicates if a port is currently operating as an edge port (or PortFast port). This will indicate Enabled if the port is in the forwarding state due to either of the following configurations:
  - The port is configured as an Edge Port and is therefore automatically in the forwarding state.
  - The port is configured as an Auto Edge port and, because it has not received BDPUs, has transitioned to forwarding state.

- **Port State**—Current STP state of a port. If enabled, the port state determines the forwarding action that is taken on traffic. Possible port states are:
  - **Disabled**—STP is currently disabled on the port. The port does not participate in the spanning tree, but is in an operational state to learn MAC addresses and forward traffic.
  - **Discarding**—Port is currently blocked and cannot be used to forward traffic or learn MAC addresses.
  - **Learning**—Port is currently in the learning mode. The port cannot forward traffic, however, it can learn new MAC addresses.
  - **Forwarding**—Port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Designated Bridge ID**—Bridge identifier of the bridge that offers the lowest root path cost to a LAN. The ID is a concatenation of the bridge priority and the base MAC address of the bridge.
- **Designated Port ID**—Port identifier on the Designated Bridge that offers the lowest root path cost to the LAN. The ID is a concatenation of the port priority and the interface number of the port.
- **Designated Cost**—The root path cost from the designated bridge to the root bridge. Ports with lower designated cost are less likely to be blocked when STP detects loops.
- **Speed**—Port speed.
- **LAG**—LAG that the port is a member of, if any.

RSTP Interface Settings

Rapid Spanning Tree Protocol (RSTP) ensures a faster convergence of a loop-free spanning tree for any bridged LAN. To display the *RSTP Interface Settings* page, click **Spanning Tree** > **RSTP Interface Settings** in the navigation window.

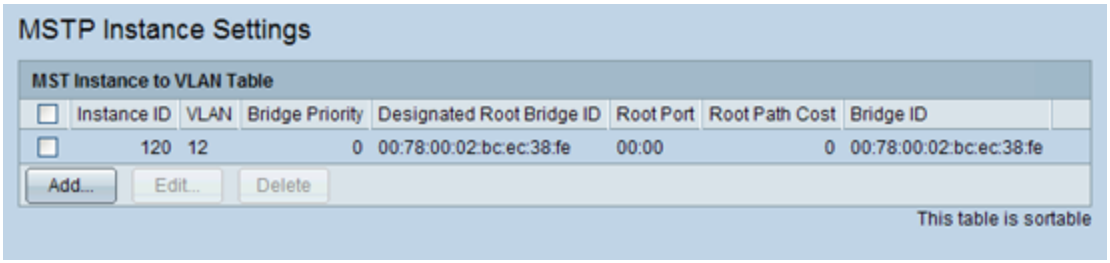
A rapid spanning tree topology is formed automatically when RSTP is selected as the spanning tree mode. Use the *STP Status & Global Settings* page to enable RSTP mode.

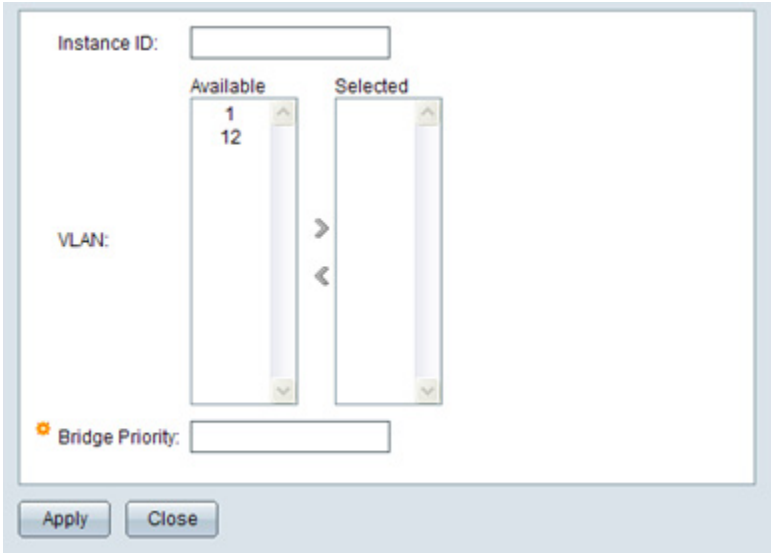
By default, the RSTP Interface Settings Table displays information for each port. Use the Interface Type list to display ports or LAGs in the table. The RSTP Interface Table displays the following information for each port:

- **Point to Point Operational Status**—A physical port has a point-to-point connection to a LAN if it operates in full duplex.
- **Port Role**—Port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
  - **Root**—Provides the lowest root path cost to the root bridge among all the ports in the switch.
  - **Designated**—Provides the lowest root path cost to the root bridge from a LAN. The switch is the designated bridge in the LAN.
  - **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 only when two ports are connected in a loop by a point-to-point link, or when a LAN has two or more connections connected to a shared segment.
  - **Disabled**—The port is not participating in the Spanning Tree.
- **Mode**—Indicates whether the RSTP administrative mode is enabled or disabled for the port.
- **Edge Port Operational Status**—If enabled for the port or LAG, the port is automatically placed in the forwarding state. See **Configuring STP Interface Settings** for instructions on modifying this setting.
- **Port Status**—The operational state of the port.

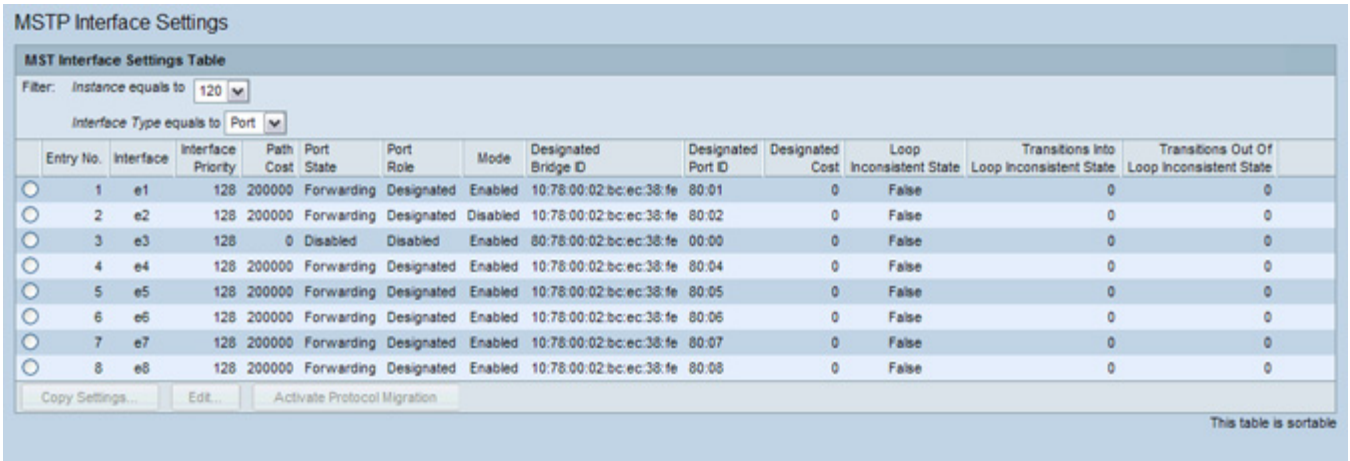
You can select a port and click **Activate Protocol Migration** to have the switch send RSTP BPDUs to the port. This can be used to test whether all legacy bridges on the LAN have been removed.

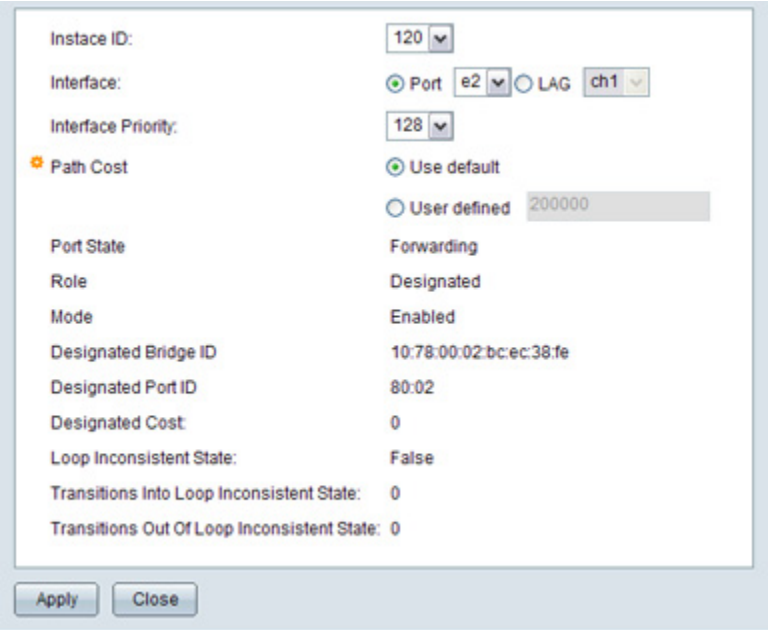
MSTP Instance Settings





MSTP Interface Settings




Instace ID:
120
Interface:
Port
e2
LAG
ch1
Interface Priority:
128
Path Cost
Use default
User defined
200000
Port State
Forwarding
Role
Designated
Mode
Enabled
Designated Bridge ID
10:78:00:02:bc:ec:38:fe
Designated Port ID
80:02
Designated Cost:
0
Loop Inconsistent State:
False
Transitions Into Loop Inconsistent State:
0
Transitions Out Of Loop Inconsistent State:
0
Apply
Close

7

MAC Address Tables

This chapter describes the static configuration and dynamic learning of Media Access Control (MAC) addresses into the filtering database of the switch. The switch searches its filtering database to determine which port a packet is to be forwarded to. The filtering database is also referred as the bridging table in this document. The search is based on the VLAN and destination MAC address of the packet. If search does not result with a matching entry, the switch floods the packets to the VLAN excluding the ingress port.

It includes the following topics:

- **Configuring Static MAC Addresses**
- **Configuring the Aging Time for Dynamic Addresses**
- **Dynamic MAC Addresses**

Configuring Static MAC Addresses

The *Static Addresses* page displays a list of MAC addresses that are manually configured into the bridging table of the switch. A static MAC address is also associated with a VLAN and a port.

To add static MAC address entries:

STEP 1 Click **MAC Address Tables** > **Static Addresses** in the navigation window.

STEP 2 Click **Add**.

STEP 3 Enter the parameters:

- **VLAN ID**—Select the VLAN in which the device with the static MAC address resides.
- **Interface**—Specify the port/LAG in which the device with the static MAC addresses can be reached.

- **MAC Address—** Enter the static MAC address.
- **Status**—Select a status for this static MAC address:
  - **Permanent**—When this status is selected, the static MAC address does not expire. Note, however, that if the switch is rebooted, the entry is not restored unless the Running Configuration file type was copied to the Startup Configuration file type. See **Copying and Saving Configuration Files**.
  - **Delete on Timeout**—When this status is selected, the static MAC address is static but may expire due to inactivity. In this respect, it is treated like a dynamically learned MAC address. See the *Dynamic Address Settings* to set the aging period.
  - **Secure**—When this status is selected, the MAC address is secured and is used in conjunction with the Port Security feature. When a MAC address is secured at a port, packets that originate from the MAC address can only be ingressed from the secured port. Otherwise, the packets are discarded. If port security is disabled on the port, the MAC address is deleted from the static MAC address list. When Port Security is enabled at a port, the port can support a maximum of 256 static and dynamic MAC addresses. (For more information, see **Enabling Port Security**).

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

NOTE To delete a static MAC address, select it in the table and click **Delete**.

Configuring the Aging Time for Dynamic Addresses

The *Dynamic Address Settings* page enables you to set an aging time, after which the system removes addresses in the dynamic MAC address table that have not been refreshed. The aging period applies to dynamically learned addresses and to static addresses that are configured to Delete on Timeout. The default aging time is 300 seconds.

To configure the aging time:

STEP 1 Click **MAC Address Tables** > **Dynamic Address Settings** in the navigation window.

STEP 2 Specify an aging time from 10 to 1,000,000 seconds.

STEP 3 Click **Apply**. Your changes are saved to the Running Configuration.

Dynamic MAC Addresses

When the switch cannot find an entry in its bridging table that matches the VLAN and the destination MAC address of an incoming packet, the switch learns the MAC address, the VLAN, and the ingress port of the packet and adds an entry to the Dynamic Address table.

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 the configured aging period (see **Configuring the Aging Time for Dynamic Addresses**).

To display the *Dynamic Addresses* page, click **MAC Address Tables** > **Dynamic Addresses** in the navigation window.

NOTE This page might take up to 45 seconds to display when the Dynamic Address Table contains the maximum number of entries.

By default, the Dynamic Address Table displays all dynamically learned MAC addresses. You can enter filter criteria and click **Go** to filter the display. Use the *VLAN ID* filter to display table entries for a particular VLAN. Use the *MAC Address* filter to display entries for a particular MAC address. Use the *Interface* filter to display entries for a particular port or LAG. Click **Clear Filter** to display all of the entries.

The Dynamic Address Table displays the following fields for each entry it learns:

- **VLAN ID**—VLAN on which the MAC address was learned. Frames are forwarded to the interface only if they are associated with this VLAN.
- **MAC Address**—The dynamically learned MAC address.
- **Interface**—The port on which the MAC address was dynamically learned. Frames specifying this MAC address and VLAN as the destination are forwarded out to this port.

Click **Clear Table** to clear all dynamic MAC address entries from the table.

8

Multicast

This chapter describes how to configure the multicast protocols that forward packets from one source to multiple destinations.

It contains the following topics:

- **Multicast Properties**
- **Configuring MAC Group Addresses**
- **Configuring Group-to-Port**
- **Configuring IGMP Snooping**
- **Configuring MLD Snooping**
- **Configuring IGMP Multicast Router Interfaces**
- **Configuring MLD Multicast Router Interfaces**

Multicast protocols deliver packets from one source to multiple receivers. They facilitate better bandwidth utilization and help to reduce the processing load on hosts and routers, making them ideal for use in applications such as video and audio conferencing, whiteboard tools, and stock distribution tickers.

The switch maintains a multicast forwarding table to make forwarding decisions for packets that arrive with a multicast destination MAC address. When multicasts are restricted only to specified ports, traffic is prevented from going to parts of the network where there are no receivers. When a packet enters the switch, the destination MAC address is combined with the VLAN ID and a search is performed in the multicast forwarding table. If no match is found, then the packet is either flooded to all ports in the VLAN or discarded, depending on the switch configuration. If a match is found, the packet is forwarded only to the ports that are members of that multicast group.

Multicast entries can be learned by *snooping* (listening in on) the layer 3 protocols that manage multicast memberships:

- IPv4 multicast group addresses can be learned through the Internet Group Management protocol (IGMP).
- IPv6 multicast group addresses can be learned through the Multicast Listener Discovery (MLD) protocol.

Interfaces with IGMP and MLD multicast routers for a specific VLAN can be either statically or dynamic configured. The multicast routers use IGMP and MLD to manage the membership of the multicast groups. A multicast router is also required in order for the switch to support IGMP/MLD snooping properly in a VLAN.

Multicast Properties

You can use the *Multicast Properties* page to specify how multicast packets are forwarded within VLANs.

When you create a VLAN, a default multicast forwarding option is assigned. You can use the Global Multicast Mode setting to set all VLANs currently configured on the switch to a selected forwarding mode. The global setting does not create a default setting for VLANs created subsequently—it simply ensures that all *existing* VLANs are configured with the specified mode. You can also configure how the switch forwards multicast packets on an individual or per-VLAN basis.

Configuring a Multicast Forwarding Mode on all VLANs

To configure all current VLANs with a particular multicast forwarding mode:

STEP 1 Click **Multicast** > **Properties** in the navigation window.

STEP 2 Select a Global Multicast Mode to apply to all VLANs. If a VLAN has been configured with a different mode, it is reset to the following mode:

- **Forward Unregistered**—If a packet is received from a VLAN with a multicast destination address and no ports in the VLAN are registered to receive multicast packets for that address, then the packet is flooded to all ports in the VLAN. The responsibility for accepting or dropping the packets belongs to the hosts. If a multicast packet is received and there are ports registered to receive it, the packet is sent only to the registered ports.

- **Forward All**—All multicast packets received from a VLAN are flooded to all ports in the VLAN, regardless of port registrations to multicast addresses.
- **Filter Unregistered**—If a packet is received from a VLAN for a multicast destination address and no ports in the VLAN are registered to receive multicast packets for that address, then the packets are dropped.

STEP 3 Click **Apply**. Your changes are saved to the Running Configuration.

Configuring Multicast Properties on an Individual VLAN

To configure a VLAN to have a different forwarding mode than the Global Multicast Mode setting:

STEP 1 Select the VLAN from the VLAN ID menu and click **Edit**.

STEP 2 Select the Multicast Mode as described in **Configuring a Multicast Forwarding Mode on all VLANs**.

STEP 3 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Configuring MAC Group Addresses

The *MAC Group Address* page enables you to view and configure associations between multicast group MAC address and VLANs on the switch. You can configure static associations or they can be learned dynamically through IGMP or MLD snooping. When a packet is received for a multicast group address that matches an entry in the MAC Group Address Table, the packet is sent only to ports that are members of the VLAN.

The switch supports up to 256 IPv4 and IPv6 MAC group address table entries, static and dynamic combined. A dynamic entry is aged out if no packets are received for the MAC group address for a configurable time (see the *IGMP Snooping* page to configure the IGMP Group Membership interval).

Viewing the MAC Group Address Table

To view the MAC Group Address Table, click **Multicast** > **MAC Group Address** in the navigation window.

By default, all entries display in the table. You can use the VLAN ID and MAC Group Address filters to display only entries that match the specified values. The following fields display:

- **Type**—Indicates whether the entry is statically configured or dynamically learned.
- **VLAN ID**—VLAN ID to which multicast packets are forwarded when they match the specified multicast MAC address.
- **MAC Group Address**—Multicast group MAC address in hexadecimal format that is compared to an incoming packet destination MAC address.

Adding a Static MAC Group Address Table Entry

To add a static multicast MAC address and associate it with a VLAN:

STEP 1 Click **Add** on the *MAC Group Address* page.

STEP 2 Enter the parameters:

- **VLAN ID**—Select a VLAN from the list.
- **Address Type**—Select IPv4 to specify an address in 32-bit IPv4 notation (xxx.xxx.xxx.xxx), or select MAC to specify the address in a 6-byte hexadecimal format (xx.xx.xx.xx.xx.xx).
- **MAC Group Address**—Enter the address in the selected format. For an IPv4 address, the least significant 23 bits are mapped to an Ethernet MAC address.

STEP 3 Click **Apply** and then click **Close**. The entry appears in the MAC Group Address Table.

Configuring MAC Address Group Port Membership

By default, packets destined to a multicast MAC address are flooded on all ports. Ports might become members of a particular MAC address group dynamically through the exchange of IGMP packets, or you can statically configure them as members.

To view details and configure the port members of a multicast group address:

STEP 1 Select an entry on the *MAC Group Address* page and click **Details**.

The page identifies the members of the multicast group address on every port.

STEP 2 Click **Static** to configure a port as a static member of the multicast MAC address. Or click **None** to remove the port as a static member of the MAC Multicast Address.

STEP 3 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Configuring Group-to-Port

The *Group to Port* page enables you to configure associations between VLANs and multicast group MAC address on the switch. You can configure static associations or they can be learned dynamically through IGMP or MLD snooping. (see the *IGMP Snooping* page to configure the IGMP Group Membership interval) The results can be displayed in the MAC Group Address Table.

To configure Group to Port:

STEP 1 Click **Multicast** > **Group to Port** in the navigation window.

STEP 2 Use the VLAN ID and MAC Group Address filters to display entries that match the specified values:

- **VLAN ID equals to**—Select the VLAN ID to which multicast packets are forwarded when they match the specified multicast MAC address.
- **MAC Group Address equals to**—Select the group MAC address that is compared to an incoming packet destination MAC address.

STEP 3 Select the Filter.

STEP 4 Set the type to indicate whether the entry is statically configured or dynamically learned. Ports can become members of a particular MAC address group dynamically through the exchange of IGMP packets, or you can statically configure them as members.

STEP 5 Click **Apply**. Your changes are saved to the Running Configuration.

Configuring IGMP Snooping

Internet Group Management Protocol (IGMP) is a layer 3 Internet protocol that enables IPv4 networks to manage memberships to multicast groups. (IPv6 multicast traffic is managed using the MLD protocol, as described in **Configuring MLD Snooping**.) IGMP communication occurs between IGMP routers and IGMP-enabled hosts (clients). Although the switch does not initiate or reply to IGMP packets, it can be configured to listen to IGMP communication between routers and clients that are connected by the switch, and to make forwarding decisions that help to reduce unnecessary network traffic.This listening behavior is referred to as IGMP snooping. This is particularly beneficial for high-bandwidth multicast network traffic.

Ordinarily, when the switch receives broadcast or multicast packets, the switch forwards a copy into each of the remaining network segments. This approach works well for broadcast packets that are intended to be processed by all connected nodes. For multicast packets, however, this approach could lead to less efficient use of network bandwidth, particularly when the packet is intended for only a small number of nodes; packets are flooded into network segments where no node has an interest in receiving the packet.

IGMP snooping enables the switch to intercept membership reports from IGMP clients and queries from routers. If the intercepted communications indicate that no IGMP clients exist on a link for a particular multicast destination address within a VLAN, then the switch does not send copies of those multicast packets to that network segment.

IGMP snooping can be enabled or disabled on each VLAN. When enabled on a VLAN, IGMP snooping is performed on all interfaces that are members of that VLAN.

Although IGMP is based on IP multicast addresses, the switch performs the actual multicast forwarding based on the equivalent MAC addresses.

To configure IGMP snooping:

STEP 1 Click **Multicast** > **IGMP Snooping** in the navigation window.

STEP 2 Select Enable for the IGMP Snooping Status.

STEP 3 Click **Add** in the IGMP Snooping Table.

STEP 4 For **VLAN ID**, select the VLAN that is to support IGMP snooping.

STEP 5 Configure the following settings:

- **IGMP Fast Leave**—Select Enable to allow the switch to immediately remove a port (or LAG) from its multicast forwarding table when it receives an IGMP leave message for that multicast group. When enabled, the switch removes the port without first sending out general queries to the interface. Enable Fast Leave mode only on VLANs where only one host is connected to each port. This prevents the inadvertent dropping of the other hosts that are connected to the same port and remain interested in receiving multicast traffic directed to that group.
- **IGMP Group Membership Interval**—Specify the time in seconds that the switch waits for an IGMP membership report from a particular group on a particular interface before deleting the interface from the multicast forwarding database entry. Select Default to specify 260 seconds, or select User Defined and enter a value in the range 2 to 3600 seconds.
- **IGMP Max Response Time**—Specify the time in seconds that the switch waits for a reply after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Group Membership Interval value. Select Default to specify 10 seconds, or select User Defined and enter a value in the range 1 to 25 seconds.
- **IGMP MRouter Expiry Time**—Specify the time in seconds that the switch waits for a query to be received on an dynamic mrouter interface before the interface is removed from the VLAN. A value of 0 indicates an infinite timeout; i.e., no expiration. Select Default to specify 0 seconds, or select User Defined and enter a value in the range 0 to 3600 seconds.

STEP 6 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

The new VLAN entry appears in the IGMP Snooping Table.

STEP 7 Ensure that an IGMP Mrouter interface has been configured for this VLAN (or all VLANs). See **Configuring IGMP Multicast Router Interfaces**.

Configuring MLD Snooping

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes wishing to receive IPv6 multicast packets) on its directly-attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP, which performs a similar function for IPv4 multicast traffic (see **Configuring IGMP Snooping**).

When MLD snooping is enabled, the switch selectively forwards IPv6 multicast packets to a list of ports that want to receive the data instead of flooding the packets to all ports in the VLAN. This list is constructed by snooping IPv6 multicast control packets.

NOTE The switch supports MLD snooping of MLD version 1 and version 2 packets. The switch can be configured to perform MLD snooping and IGMP snooping simultaneously.

MLD snooping can be enabled or disabled separately on each VLAN. Although MLD is based on IPv6 addresses, the switch performs the actual multicast forwarding based on the equivalent MAC addresses.

To enable and configure MLD snooping:

STEP 1 Click **Multicast** > **MLD Snooping** in the navigation window.

The MLD Snooping Table lists each VLAN on which this feature is enabled.

STEP 2 Select Enable for the MLD Snooping Status.

STEP 3 Click **Add** in the MLD Snooping Table.

STEP 4 For **VLAN ID**, select the VLAN that is to support MLD snooping.

STEP 5 Enter the parameters:

- **MLD Fast Leave Mode**—Select Enable to allow the switch to immediately remove a port (or LAG) from its multicast forwarding table when it receives an MLD leave message for that multicast group. When enabled, the switch removes the port without first sending out MAC-based general queries to the interface. Enable Fast Leave mode only on VLANs in which only one host is connected to each port. This prevents the inadvertent dropping of the other hosts that are connected to the same port and remain interested in receiving multicast traffic directed to that group.
- **MLD Group Membership Interval**—Specify the time in seconds that the switch waits for an MLD membership report from a particular group on a particular interface before deleting the interface from the multicast forwarding database entry. Select Default to specify 260 seconds, or select User Defined and enter a value in the range 2 to 3600 seconds.
- **MLD Max Response Time**—Specify the time in seconds that the switch waits for a reply after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the MLD Group Membership Interval value. Select Default to specify 10 seconds, or select User Defined and enter a value in the range 1 to 65 seconds.
- **MLD Mrouter Expiry Time**—Specify the time in seconds that the switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with an MLD multicast router attached. A value of 0 indicates an infinite timeout; i.e., no expiration. Select Default to specify 0 seconds, or select User Defined and enter a value in the range 0 to 3600 seconds.

STEP 6 Click **Apply** and then click **Close**.

The new VLAN entry appears in the MLD Snooping Table.

STEP 7 Ensure that an MLD Mrouter interface has been configured for this VLAN. See **Configuring MLD Multicast Router Interfaces**.

Configuring IGMP Multicast Router Interfaces

An IGMP router must exist to manage the IGMP clients in a VLAN. For each VLAN that supports IGMP snooping, the switch must be statically configured with or must dynamically learn one or more interfaces where there is an IGMP router. An interface that has an IGMP router is known a IGMP Multicast router Interface. A VLAN that is IGMP snooping-enabled must have one or more IGMP multicast router interfaces. An IGMP multicast router can serve one or more VLANs.

To enable a switch port or LAG as an IGMP Mrouter interface and to configure related settings:

STEP 1 Click **Multicast** > **IGMP Mrouter** in the navigation window

By default, the IGMP MRouter Table lists each switch port. To show LAGs, select LAG from the Interface Type list.

STEP 2 Select the port or LAG that you want to configure and click **Edit**.

STEP 3 Select Enable for the Mode.

STEP 4 To specify the VLANs that use this interface as the IGMP Mrouter interface, move the VLAN to the Selected list, as described below.

- To select a VLAN: Click a VLAN in the Available list, and then click the right-arrow button to move it to the Selected list.
- To remove a VLAN: Click a VLAN in the Selected list, and then click the left-arrow button to move it to the Available list.

STEP 5 Click **Apply** and then click **Close**.

In the IGMP Mrouter Table, the interface displays Enable in the Mode column and lists the selected VLANs.

Configuring MLD Multicast Router Interfaces

An MLD multicast router must exist to manage the MLD clients in a VLAN. For each VLAN that supports MLD snooping, the switch must be statically configured with or dynamically learn one or more interfaces where there is an MLD multicast router. The interface that has an MLD router is known a MLD Multicast router Interface. A VLAN that is MLD snooping-enabled must have one or more MLD multicast router interfaces. An MLD multicast router can serve one or more VLANs.

To enable a switch port or LAG as an MLD Mrouter interface:

STEP 1 Click **Multicast** > **MLD Mrouter** in the navigation window.

By default, the MLD MRouter Table lists each switch port. To show LAGs, select LAG from the Interface Type list.

STEP 2 Select the port or LAG to configure and click **Edit**.

STEP 3 Select Enable for the Mode.

STEP 4 Move VLAN IDs between the Available and Selected lists. VLANs in the Selected list use this port or LAG as the MLD Mrouter interface.

- To select a VLAN: Click a VLAN in the Available list, and then click the right-arrow button to move it to the Selected list.
- To remove a VLAN: Click a VLAN in the Selected list, and then click the left-arrow button to move it to the Available list.

STEP 5 Click **Apply** and then click **Close**.

In the MLD Mrouter Table, the interface displays Enable in the Mode column and lists the included VLANs.

9

IP Configuration

This chapter describes the Address Resolution Protocol (ARP) and Domain Name System (DNS) client features.

It includes the following topics:

- **ARP Table**
- **Domain Name System**

ARP Table

The switch maintains an Address Resolution Protocol (ARP) Table. Each entry in the table includes the IP address and the MAC addresses of a device that has recently communicated with the switch.

You can use the *ARP* page to display ARP entries learned by the management VLAN. To display this page, click **IP Configuration** > **ARP** in the navigation window.

You can click **Clear ARP** to delete all entries from the table, except for the management port IP address and MAC address.

Domain Name System

The switch supports IPv4 DNS client functionality. When enabled as a DNS client, the switch provides a hostname lookup service to other applications on the switch such as ping, RADIUS, syslog, Auto Configuration, and TFTP. The switch can be configured with DNS servers that resolve hostnames to IP addresses. The switch can also be configured with static host-name-to-IP-address mappings that bypass the DNS server.

See the following topics for more information on the configuration pages available in the **IP Configuration** > **Domain Name System** menu.

- **Configuring DNS Servers**
- **Hostname Mapping**

Configuring DNS Servers

To resolve a hostname to an IP address, the client contacts one or more DNS servers. DNS servers can be learned dynamically if the management interface is configured as a DHCP client (see **Management Interface**). You can also use the *DNS Servers* page to statically configure DNS servers.

DNS client functionality is enabled by default.

Configuring Global DNS Settings

To configure the DNS server mode and global settings:

STEP 1 Click **IP Configuration** > **Domain Name System** > **DNS Servers** in the navigation window.

STEP 2 Select Enable to implement DNS client functionality on the switch, if it is not already enabled.

STEP 3 Enter the following parameters:

- **Default Domain Name**—Specify a domain name to be used to complete an unqualified hostname. For example, *finance.yahoo.com* is a fully qualified domain name. If only the unqualified hostname, *finance,* is specified, the default domain name *yahoo.com* would be appended, with a period in between. In your entry, do not include the period that separates the unqualified hostname from the domain name. The range is 1–255 alphanumeric characters.
- **Domain retry**—Specify the number of times to retry sending DNS queries. The range is 0–100 and the default value is 2 times.
- **Domain timeout**—Specify the time in seconds that the switch waits for a response to a DNS query. The range is 0–3600 seconds and the default is 3 seconds.

NOTE: Default domain names may be learned from reply messages from a DHCP server. These names display in the Default Domain Name List.

STEP 4 Click **Apply**. Your changes are saved to the Running Configuration.

Adding DNS Servers

The DNS Servers Table lists the configured servers.

To add a DNS server:

STEP 1 Click **Add**.

STEP 2 Specify the DNS server IPv4 or IPv6 address.

STEP 3 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration and the server appears in the DNS Servers Table.

Hostname Mapping

Use the *Host Mapping* page to view and configure associations between hostnames and IP addresses. You can statically associate a hostname with an IP address. You can also view hostnames that have been learned dynamically through applications that use the DNS lookup service.

NOTE If you configure a static hostname and IP address, and that same hostname IP address mapping is later learned from DNS, the entry becomes dynamic and it is no longer saved as a static entry in the the Running Configuration.

Configuring Static DNS Mappings

The Host Mapping Table lists hostnames that are statically assigned to IP addresses on the switch. To configure a static hostname mapping:

STEP 1 Click **IP Configuration** > **Domain Name System** > **Host Mapping** in the navigation window.

STEP 2 Click **Add**.

STEP 3 Enter a hostname from 1–255 alphanumeric characters. The hostname must begin with a letter.

STEP 4 Enter an IPv4 or IPv6 address to be associated with the hostname.

STEP 5 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Viewing and Deleting Dynamic DNS Entries

The DNS Dynamic Entries table displays hostnames that have been learned by applications that use DNS lookup services. For example, if you ping a hostname, the DNS lookup service is invoked and an associated IP address is learned and added to the table.

The DNS Dynamic Entries table displays the following fields:

- **Hostname**—Host name assigned to the IP address (or to an official hostname).
- **Total**—Number of minutes the hostname has been reserved for this assignment.
- **Elapsed**—Number of minutes that have elapsed since the hostname was assigned.
- **Type**—Identifies the hostname as one of the following:
  - **IP Address**—The assigned hostname is associated with an IP address.
  - **Canonical**—The assigned hostname is an alias or nickname for a properly denoted (official) hostname. For example, *www.google.com* might be a hostname alias associated with the official hostname *www.l.google.com*.
- **Addresses**—If the Type is IP, this field displays the IPv4 address or the IPv6 address that is associated with the hostname. If the Type is Canonical, this field displays the canonical hostname that the alias is associated with. A canonical DNS address might have more than one hostname alias associated with it.

To delete a dynamic entry, select it and click **Delete**. To delete all dynamic entries from the table, click **Delete All Dynamic Entries**.

10

Security

This chapter describes the security features for the port, user, and server.

It includes the following topics:

- **RADIUS**
- **Password Strength**
- **Management Access Profile Rules**
- **Authentication Methods**
- **Storm Control**
- **Port Security**
- **802.1X**

RADIUS

The switch supports Remote Authorization Dial-In User Service (RADIUS) client functionality. RADIUS has become the protocol of choice by administrators of large accessible networks for authenticating users prior to access. To authenticate users in a secure manner, a RADIUS client and RADIUS server are configured with the same shared password or *secret*. This secret is used to generate one-way encrypted authenticators that are present in all RADIUS packets. Without knowledge of the secret, the possibility of a malicious user correctly spoofing packets is sufficiently reduced.

The RADIUS client on the switch is used for switch management access authentication and IEEE 802.1X (dot1X) port access control (see **Management Access Profile Rules** and **802.1X**).

You can use the *RADIUS* page to configure global RADIUS settings and add RADIUS servers.

Configuring Global RADIUS Settings

To configure the global settings:

STEP 1 Click **Security** > **RADIUS** in the navigation window.

STEP 2 Enter the parameters:

- **Retries**—Maximum number of times the RADIUS client retransmits requests to the RADIUS server. The range is 1 to 10. The default is 3.
- **Timeout for Reply**—Number of seconds the switch waits for a RADIUS server to reply to a server request before sending another request. The range is 1 to 30. The default is 3.
- **Dead Time**—Length of time a RADIUS server is bypassed once the switch determines it is unavailable. Bypassing unavailable switches improves switch response times. The range is 0 to 2000. The default is 0.
- **RADIUS Attribute 4** (NAS-IP Address)—Select to enable the switch to include the network access server (NAS) attribute in Access Request RADIUS server packets. If this option is disabled, the RADIUS client uses the switch management port address as the NAS-IP Address.
- **NAS-IP Address**—IP address to include in Access Request packets. This field is editable only when RADIUS Attribute 4 is enabled. The address should be unique to the NAS within the scope of the RADIUS server.

NOTE: The Current RADIUS Server field displays the IP address of the most recently configured RADIUS server, if any.

STEP 3 Click **Apply**. Your changes are saved to the Running Configuration.

Adding a RADIUS Server

You can configure multiple RADIUS servers and configure priority levels that determine the order they are contacted.

CAUTION All management users are created with read-write permissions. Ensure that all RADIUS server users you configure have the same privilege levels; otherwise they are not granted access to the switch.

To add a RADIUS Server to the RADIUS Table:

STEP 1 Click **Add**

STEP 2 Enter the parameters:

- **RADIUS Server**—IP address or hostname of the server.
- **Priority**—The lower the priority number value, higher the priority of the server. For example, server configured with priority value 1 has higher priority than server configured with priority value 2. If all the servers are configured with the same or the default priority value, the switch tries the RADIUS servers in a first-come, first served basis. The range is 1 to 65535. The default is 8.
- **Key String**—A shared secret text string used for authenticating and encrypting all RADIUS communications between the switch and the RADIUS server. This secret must match the secret configured on the RADIUS server. This must be an ASCII alphanumeric value between 32 to 176 characters.
- **Authentication Port**—Port number used for RADIUS authentication requests and replies. The default port, 1812, is the well-know IANA port number for RADIUS authentication services. The range is 1025 to 65535. The default is 1812.
- **Message Authenticator**—This field is selected by default. When enabled, the message authenticator attribute is included in RADIUS request messages to the server. This attribute protects the RADIUS messages from spoofing and tampering. The shared secret is used as the key. If the RADIUS Message Authenticator attribute is present in the packet, it is verified by the server. If verification fails, the server drops the request packet.

STEP 3 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Password Strength

You can use the *Password Strength* page to configure characteristics of secure management user passwords.

To configure password strength settings:

STEP 1 Click **Security** > **Password Strength** in the navigation window.

STEP 2 Enter the following parameters:

- **Strength Check**—Select Enable to configure the types of checks to be performed:
- **Minimum Password Length**—The minimum number of characters required for a management user password. Set the minimum password length to a value in the range of 0–64 characters.
- **Password Aging Time**—Select the checkbox and enter the time after which a password expires, from 1–365 days. When a password ages out, the user must chose a new password before continuing.
- **Password Exclude Keyword Check**—Select Enable to check for preconfigured keywords in a password when a user attempts to create or change the password. The preconfigured keywords are *cisco* and *ocsic*.
- **Password User Name Check**—Select Enable to prevent users from including their user name in their password when they create or change it.
- **Character Can Repeat Itself Consecutively a Maximum of 3 Times**—Select Enable to have the switch check whether any character in the password is repeated consecutively more than three times.
- **Minimum Number of Character Classes**—Select the checkbox and enter the minimum number of character classes that must be represented in the password string. The four possible character classes are: uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard.

STEP 3 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Management Access Profile Rules

Use the *Management Access Profile Rules* page to define a profile and rules for accessing the device for management purposes.

You can limit access to specific user names, ingress ports or LAGs, and source IP addresses.

To display this page, click **Security** > **Management Access Profile Rules** in the navigation window.

The Access Profile Table lists the profile name of the currently configured profile, if one exists. The Profile Rule Table shows the existing rules for the profile. By default, no access profiles and rules are configured on the switch. You can create and enable only one profile and all the rules you create are assigned to that profile.

Configuring an Access Profile and Rules

To create an access profile and assign rules to it:

STEP 1 In the Access Profile Table, click **Add**.

STEP 2 Specify the Access Profile Name and select Enable.

STEP 3 Click **Apply** and then click **Close**.

The new profile appears in the Access Profile Table. Next, add the rules to the profile.

STEP 4 In the Profile Rule table, click **Add**.

STEP 5 Specify any of the following parameters to restrict or allow access:

- **Rule Priority**—The rules are validated against the incoming management request in the ascending order of their priorities. If a rule matches, the specified action is performed and rules below are ignored. For example, if you configure Source IP 10.10.10.10 with priority 1 to Permit, and configure Source IP 10.10.10.10 with priority 2 to Deny, then access is permitted to this IP address when the profile is active, and the second rule is ignored. The range is 1 to 16, with 1 having the highest priority.

To limit access to the web-based switch configuration utility only to specified users, for example, you can create a rule in which HTTP access is denied to all users, and then create another rule in which specific users are permitted. The rule that permits the specific users must have a higher Rule Priority than the rule that denies all users.

CAUTION: If a profile is activated that denies access to an intranet or domain where a current web management session is active, the session remains active until logout or timeout. Future sessions are blocked by the profile. Active sessions using Internet Explorer 8 are terminated immediately unless the switch management IP address is added to the Local Intranet Sites list in Internet Explorer. See **Starting the Web-Based Switch Configuration Utility** for instructions.

- **Action**—Select the action to be performed when the rules criteria is matched.
  - **Permit**—The specified interface, user, or IP address is permitted access to the switch that would otherwise be explicitly forbidden by a deny rule.
  - **Deny**—The specified interface, user, or IP address is denied access to the switch.
- **Applies to Interface**—Select All to apply this rule to all interfaces (ports and LAGs). Or, select User Defined and select the port or LAG that the rule applies to.
- **Applies to User**—Select All to apply this rule to all system users. Or, select User Defined and select a User Name that the rule applies to.
- **Applies to Source IP Address**—Select All to apply the rule to any source IP addresses. Or select User Defined and specify a source IPv4 address and mask that this rule applies to.

STEP 6 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

The new rule appears in the Profile Rule Table. You can select the rule and click **Edit** to modify it or click **Delete** to remove it from the access profile.

NOTE User **cisco** will not be denied management access.

Modifying and Deleting Access Profiles and Rules

Before you can delete an Access Profile or modify the rules, you must disable the profile.

To disable an access profile:

STEP 1 Select the profile in the Access Profile Table and click **Edit**.

STEP 2 Uncheck the Enable box.

STEP 3 Click **Apply**, and then click **Close**.

When you finish making changes, re-enable the access profile.

To delete an access profile (after disabling it):

STEP 1 Select the profile in the Access Profile Table.

STEP 2 Click **Delete**.

To delete a profile rule (after disabling the access profile):

STEP 1 Select the rule in the Profile Rule Table.

STEP 2 Click **Delete**.

To modify a profile rule (after disabling the access profile):

STEP 1 Select the rule in the Profile Rule Table and click **Edit**.

STEP 2 Enter the new settings.

STEP 3 Click **Apply**, and then click **Close**.

To enable an access profile (after completing all changes):

STEP 1 Select the profile in the Access Profile Table and click **Edit**.

STEP 2 Check the Enable box.

STEP 3 Click **Apply**, and then click **Close**.

Authentication Methods

You can use the *Authentication Methods* page to specify how users are allowed access to switch ports.

To select the authentication method:

STEP 1 Click **Security** > **Authentication Methods** in the navigation window.

STEP 2 an authentication method from the list:

- **Local**—A user ID and password combination from the supplicant is compared with a locally-stored user database on the switch.
- **None**—No authentication method is used.
- **RADIUS**—Authentication requests are passed to a RADIUS server that replies with RADIUS Access-Accept or Access-Reject frames. If the switch cannot reach the server, the request is denied.
- **RADIUS, None**—Authentication requests are passed to a RADIUS server that replies with RADIUS Access-Accept or Access-Reject frames. If the switch cannot reach the server, then no authentication method is used and the request is accepted.
- **RADIUS, Local**—Authentication requests are passed to a RADIUS server. If the switch cannot reach the server, the local user database is used to accept or reject the request.

  NOTE When the (Radius, None) or the (Radius, Local) option is selected, None or Local is used only if the Radius Server specified is incorrect or it is not specified; if it is correct, but the credentials are incorrect, the authentication fails and does not fall back to the None or the Local option.

STEP 3 Click **Apply**. Your changes are saved to the Running Configuration.

Storm Control

A traffic storm is the result of an excessive number of broadcast, multicast, or unknown unicast messages simultaneously transmitted across a network by a port. Forwarded message responses might create a loop and overload network resources and cause the network to time-out.

The switch measures the incoming broadcast, multicast, or unknown unicast packet rate per port and discards packets when a rate exceeds a defined value. Storm control can be enabled or disabled on each interface.

Storm control is disabled by default on all ports for all packet types. Use the *Storm Control* page to enable and configure storm control on the switch ports.

To display and configure storm control settings for a port:

STEP 1 Click **Security** > **Storm Control** in the navigation window.

STEP 2 Select the port to configure and click **Edit**.

STEP 3 For broadcast, multicast, and unicast traffic, specify the following storm control parameters for the selected port:

- **Mode**—Select Enable to turn on storm control protection for the traffic type.
- **Rate Threshold Type**—Select the measurement the switch uses to determine whether traffic exceeds the threshold:
  - **Percent**—Traffic is dropped when it exceeds a percentage of the total capability of the link.
  - **pps** (packets per second—Traffic is dropped when it exceeds the set number of packet-per-second on the link for this type of traffic.
- **Rate Threshold**—Specify the maximum rate at which this type of packet is forwarded. If the Rate Threshold Type is Percent, enter a percentage of the total port capability (0–100 percent). If the Rate Threshold Type is pps, enter a packet per second rate (0–14880000). Ports that operate at 10 Mbps, 100 Mbps, or 1000 Mbps have a maximum throughput of 14880, pps 148800 pps, or 1488000 pps correspondingly.

NOTE: The actual rate of ingress traffic required to activate Storm Control is based on the actual size of incoming packets and the hard-coded average packet size (512 bytes) parameter. A packet-per-second rate is calculated, as the switch requires a pps value to execute or not execute storm control versus an absolute data rate measured in kilobits-per-second (kbps). For example, if the configured pps limit for broadcast packets is 10 percent, this value is converted to approximately 20000 pps for a 100 Mbps port.

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Port Security

You can enable port security on a per-port basis. When a port is secured (locked), the switch forwards only those packets with a source MAC address that is secured at the port. All other packets are discarded. This includes discarding any packet from a port with a source MAC address that is secured at another port.

A secure MAC address can be statically configured or dynamically learned. The maximum number of secure MAC addresses at a secured port is 256. Static secure MAC addresses are configured using the *Static Addresses* page. Both static and dynamic secure MAC addresses are subject to aging limits (see **Configuring the Aging Time for Dynamic Addresses**).

To display the *Port Security* page, click **Security** > **Port Security** in the navigation window.

The Port Security Table shows the current security configuration for each port. You can select LAG from the *Interface Type* list to display data for LAGs only. By default, port security is disabled globally and on each interface.

Enabling Port Security

To configure port security:

STEP 1 On the *Port Security* page, select Enable for the global Admin Mode and click **Apply**.

STEP 2 Select the port or LAG to configure and click **Edit**.

STEP 3 Configure the following settings:

- **Interface Status**—Select Lock to enable port security on the interface. When an interface transitions from unlocked to locked, all addresses that had been dynamically learned by the switch on that port are removed from its MAC address list.
- **Max No. of Static MAC Addresses**—Specify the maximum number of static secure MAC addresses at the port/LAG. Static secure MAC address are configured on the *Static Addresses* page. The total number of secure addresses cannot exceed 256.
- **Max No. of Dynamic MAC Addresses**—Specify the maximum number of dynamic secure MAC addresses that can be learned from the port/LAG. The total number of secure addresses cannot exceed 256.

  When port-security is enabled on a port, and static or dynamic limits are set to new values, the following rules apply:

  - If the new value is greater than the old value, no action is taken for either the dynamic or static addresses.
  - If the new value is less than the old value, the following actions are taken:

    Dynamic Addresses—The switch initiates a flush of all learned addresses on the port.

    Static Addresses—The switch retains the static addresses (up to the static limit) regardless of whether the addresses are configured as secure, permanent, or delete on timeout. It then deletes the remaining static addresses from the MAC address table.
- **Action on Violation**—Select how the switch handles incoming packets that are not allowed on the locked port:
  - **Discard**—Packets are dropped.
  - **Forward**—Packets are forwarded, but the source MAC addresses are not added to the forwarding database.
  - **Shutdown**—Packets are discarded and the port is shut down.
- **Trap Frequency**—Specify the number of seconds between traps when a locked port receives incoming packets that are not allowed on the port. This field displays only when the Action of Violation field is set to Discard with Trap.
- **Convert dynamic addresses to static**—Select Enable to convert all dynamic secure MAC addresses to static secure MAC addresses.

- **Reset Port**—Select to reset the port if it has been shut down by the Port Security feature.

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Viewing and Configuring Secure MAC Addresses

To view the current list of secure MAC addresses, associated ports, and VLANs, click **Secure Address Table** on the *Port Security* page.

For each interface, the Secure Address Table lists each secured statically configured MAC address, regardless of the locked or unlocked status of the port. The table also lists dynamically learned MAC addresses for locked ports. Dynamic entries for a port are cleared when the port is changed from locked to unlocked or when the link goes down.

You can click **Static Address Table** to display the page for configuring static addresses. See **Configuring Static MAC Addresses**. Be sure to set the Status field for the entry to Secure.

You can click **Port Security Table** to redisplay the Port Security page.

802.1X

Local Area Networks (LANs) are often deployed in environments that permit unauthorized devices to be physically attached to the LAN infrastructure, or permit unauthorized users to attempt to access the LAN through equipment already attached. In such environments, it might be desirable to restrict access to the services offered by the LAN to those users and devices that are permitted to use those services.

Port-based access control provides a method for networks to control whether hosts can access services provided by a connected port. You can configure the switch to use port-based network access control based on the IEEE 802.1x protocol.

The 802.1x protocol defines three types of entities:

- Supplicant: An entity that requests access to a port at the remote end of the link. The supplicant provides credentials to the network that another node

on the network—the authenticator—uses to request authentication from a server.

- Authenticator: An entity that facilitates the authentication of the supplicant on the remote end of a link. An authenticator grants port access to a supplicant if the authentication succeeds.
- Authentication Server: A server, such as a RADIUS server, that performs the authentication on behalf of the authenticator, and indicates whether the supplicant is authorized to access services provided via the authenticating port.

In the authentication process, 802.1X supports Extensible Authentication Protocol (EAP) over LANs (EAPOL) message exchanges between supplicants and authenticators.

A switch port can be configured either as an authenticator or a supplicant, but not both.

See the following topics for more information on the configuration pages available in the Security > 802.1X menu.

- **Defining 802.1X Properties**
- **Modifying Port PAE Capabilities**
- **Configuring Port Authentication**
- **Configuring Supplicant Port Authentication**
- **Displaying Authenticated Hosts**

Defining 802.1X Properties

Use the *802.1X Properties* page to configure the global 802.1X administrative mode on the switch.

To enable 802.1X security globally:

STEP 1 Click **Security** > **802.1X** > **Properties** in the navigation window.

STEP 2 Select Enable for the Port Based Authentication State to allow 802.1X port-based authentication globally on the switch.

STEP 3 Select an authentication method from the Authentication Method list:

- **None**—No authentication method is used.

- **Local**—The switch performs local authentication of a remote supplicant based on EAP-MD5. The supplicant identification must be one of the management users configured on the switch (see **Managing User Accounts**).
- **RADIUS**—The switch depends on one or more external RADIUS servers to perform the authentication. You must configure the supplicant identity and authentication directly the servers. (See **RADIUS** for information.)
- **RADIUS, None**—The switch depends on one or more external RADIUS servers to perform the authentication. (See description of RADIUS above.) If the switch cannot reach any servers, then no authentication is used.
- **RADIUS, Local**—The switch depends on one or more external RADIUS servers to perform the authentication (see description of RADIUS above.) If the switch cannot reach any servers, it performs the authentication locally (see previous description of Local).

  NOTE When the (Radius, None) or the (Radius, Local) option is selected, None or Local is used only if the Radius Server specified is incorrect or it is not specified; if it is correct, but the credentials are incorrect, the authentication fails and does not fall back to the None or the Local option.

STEP 4 Click **Apply**. Your changes are saved to the Running Configuration.

NOTE See **Modifying Port PAE Capabilities** for instructions on selecting the role for individual ports, and **Configuring Port Authentication** for instructions on configuring authentication on individual ports.

Modifying Port PAE Capabilities

Use the *Port PAE Capabilities* page to view and configure each port's 802.1X role as authenticator or supplicant.

To modify the role of a port as an authenticator or supplicant:

STEP 1 Click **Security** > **802.1X** > **Port PAE Capabilities** in the navigation window.

STEP 2 Select the port to configure and click **Edit**.

STEP 3 Select the role for the port:

- **Authenticator**—Select this option if the port must authenticate the remote supplicant before granting access to a local port.
- **Supplicant**—Select this option if the port must be connected to an authenticator and ask permission from the remote authenticator before accessing a remote port. When a port is acting as a Supplicant, the user name and password defined in the User Accounts list of the switch must be entered in the Radius Server for the authentication to succeed.

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Configuring Port Authentication

Use the *Port Authentication* page to configure port access control on ports that serve as authenticators. By default, all ports are set to Authenticator. To enable a port as an authenticator, see **Modifying Port PAE Capabilities**.

To edit a port authenticator settings:

STEP 1 Click **Security** > **802.1X** > **Port Authentication** in the navigation window.

The Port Authentication Table displays the current configuration of each port.

STEP 2 Select the port to configure and click **Edit**.

STEP 3 Enter the parameters:

- **Local Database User Name**—Use the left and right arrows to move the configured management users to the Available or Selected lists. Only users in the Selected list have access to the port, subject to authentication. This list is applicable only when the authentication is local, and not when a RADIUS server is used for authentication.
- **Current Port Control**—The current authorization status of the port (Authorized or Unauthorized).
- **Administrative Port Control**—Select the port authorization mode. The possible values are:
  - **Force Unauthorized**—Select this option to always deny port access by supplicants attaching to the port. If selected, the port control status becomes Unauthorized.

- **auto**—Select this option if the port control is based on the result of the authentication process. If the supplicant is authenticated, the port control status becomes Authorized, meaning the supplicant is granted access to the port. If the supplicant is not authenticated, the port control status becomes Unauthorized, meaning the supplicant is denied access.
- **Force Authorized**—Select this option to always allow port access if authentication of remote supplicants is not required. If selected, the port control status will be Authorized.

- **Periodic Reauthentication**—Select this option if the port is to re-authenticate its supplicant periodically. The port will reauthenticate at the scheduled interval, even if it has remained authenticated.
- **Reauthentication Period**—The interval between reauthentication attempts. The range is 300–65535 seconds. The default is 3600 seconds.
- **Reauthenticate Now**—Forces immediate port reauthentication, when selected.
- **Authenticator State**—The current port authorization state. Possible states are: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, Force Authenticate, and Force Unauthenticate.
- **Quiet Period**—Amount of time that the switch remains in the quiet state following a failed authentication exchange. During the quiet period, the switch does not accept or initiate authentication requests. Change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers. To provide a faster response time to the user, enter a smaller number than the default (60 seconds). The range is 0–65535 seconds.
- **Resending EAP**—The amount of time that lapses before EAP requests are resent. The range is 1–65535 seconds and the default is 30 seconds.
- **Supplicant Timeout**—The amount of time that lapses before EAP requests are resent to supplicants. Change the default value of this command (30 seconds) only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers. To provide a faster response time to the user, enter a smaller number than the default. The range is 1–65535 seconds.
- **Server Timeout**—The amount of time that lapses before the switch resends a request to the authentication server. The range is 1–65535 seconds and the default is 30 seconds.

- **Max EAP Requests**—The preconfigured maximum number of times the switch can send an EAP request before restarting the authentication process if it does not receive a response.
- **Termination Cause**—The reason for termination.

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Configuring Supplicant Port Authentication

Use the *Supplicant Port Authentication* page to configure port access control on ports that are configured in the supplicant role. To enable a port as an supplicant, see **Modifying Port PAE Capabilities**.

To configure supplicant port authentication:

STEP 1 Click **Security** > **802.1X** > **Supplicant Port Authentication** in the navigation window.

STEP 2 Select the port to configure and click **Edit**.

The Current Port Control field shows the current authorization mode for the port.

STEP 3 Configure the following:

- **Administrative Port Control**—Select the port authorization mode. The possible values are:
  - **Force Unauthorized**—Denies the selected interface system access by moving the interface into unauthorized state.
  - **Auto**—The switch detects the mode of the interface based on the outcome of authentication exchanges between the supplicant, the authenticator, and the authentication server.
  - **Force Authorized**—The port is placed into an authorized state without requiring authentication with the authentication server. The interface sends and receives normal traffic without client port-based authentication.

- **User Name**—Select the user to be used by the port to identify itself as a supplicant. The user must be one of the switch management users configured in the switch. The password configured for the user will be used in the authentication process. As a supplicant, the switch supports EAP-MD5 authentication method. (See **Managing User Accounts** to set up the users.)

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Displaying Authenticated Hosts

To display ports that have authenticated users on the *Authenticated Hosts* page, click **Security** > **802.1X** > **Authenticated Hosts** in the navigation window.

The Authenticated Hosts Table displays the following information for each host:

- **Port**—Port used for authentication.
- **User Name**—User name of the host.
- **Supplicant MAC Address**—Supplicant device MAC address.
- **Session Time**—Time since the supplicant logged in.
- **Session Timeout**—Time that the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port.
- **Authentication Method**:
  - **Local**—A user ID and password combination from the supplicant was compared with a locally-stored user database on the switch. Or the switch could not reach a server and the local user database was used to accept or reject the request.
  - **None**—No authentication method was used. Or the switch attempted to could not reach the server, and no authentication method was used and the request was accepted.
  - **RADIUS**—Authentication requests are passed to a RADIUS server that replies with RADIUS Access-Accept or Access-Reject frames. If the switch cannot reach the server, the request is denied.

11

Quality of Service

This chapter describes the QoS features of the device.

- QoS Properties
- Defining Queues
- Mapping CoS/802.1p Priorities to Queues
- Mapping IP Precedence to Queues
- Mapping DSCP Values to Queues
- Defining Rate Limit Profiles
- Applying Rate Limit Profiles to Interfaces
- Traffic Shaping

QoS is a means of providing consistent, predictable data delivery by distinguishing packets that have strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given special treatment in a QoS-capable network.

Each physical port on a switch has one or more queues for transmitting packets to the attached network. Multiple queues per port are often configured to give preference to certain packets over others based on a user-defined criteria. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and, possibly, the amount of traffic present in the other queues for the port.

If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission. If a queue is full, packets have no place to be held for transmission and might be dropped by the switch.

In networks where QoS operation is enabled, all elements of the network must be QoS-capable. The presence of one or more nodes that are not QoS-capable creates a deficiency in the network path and the performance of the entire packet flow is compromised.

The switch supports four egress queues for each port or LAG. Queue 1 has the lowest priority and queue 4 has the highest priority.

The pages in the Quality of Service menu enable you to define the properties of the queues, and to associate to the queues the traffic that has particular characteristics or arrives on specific interfaces. You can also create rate limit profiles that define criteria for determining if a port is receiving more traffic than it can handle. You can then assign the rate limit profiles to ports.

QoS Properties

You can configure switch ports to assign traffic to egress queues based on the priority information encoded in Ethernet frames or IP packet headers. Or traffic might use a default priority value configured on the port where it arrives. When a port is configured to use the encoded priority value [such as the 802.1p, IP precedence, or DSCP (Differentiated Services Code Point) value], it is considered a *trusted* port. A port that is configured to use its own priority value, rather than the value encoded in the frame or packet, to make queue assignment decisions is considered *untrusted*.

If a port is configured as trusted but the frame or packet does not have priority information, the default port priority is assigned to the packet. The default port priority is zero.

You can use the *Interface Settings* page to change the value of the VLAN Priority.

You can use the *QoS Properties* page to define a port as trusted or untrusted and to configure which priority values it trusts.

To configure the trust mode on a port or LAG:

STEP 1 Click **Quality of Service** > **QoS Properties** in the navigation window.

STEP 2 Select a filter from the Interface Type menu to display ports or LAGs in the Trust Mode Configuration Table.

STEP 3 Select the interface to configure and click **Edit**.

STEP 4 To specify the type of priority values to use to determine the egress queues of the packets, select one of the following trust modes:

- **untrusted**—The port assigns its own default 802.1p priority (0).
- **trust dot1p**—The port uses the 802.1p priority value in VLAN-tagged Ethernet frames. For untagged frames, the default priority is assigned.

- **trust ip-precedence**—The port uses the IP Precedence value in the IP packet header. If no value is provided, the default priority is assigned. Non-IP VLAN tagged and untagged frames are assigned the default priority.
- **trust ip-dscp**—The port uses the DSCP marking in the IP packet header for both VLAN tagged and untagged IP packets. Non-IP VLAN tagged and untagged frames are assigned the default priority.
- **trust all**—For IP packets, the port uses the DSCP marking to determine the priority. For non-IP frames, the port uses the 802.1p priority if the frame is VLAN-tagged and the port default priority if the frame is not VLAN tagged.

STEP 5 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Defining Queues

You can use the *Queue* page to configure how the traffic scheduler determines which queue has access to the egress port. A queue can be configured in strict priority mode or Weighted Round-Robin (WRR) mode. By default, all queues are strict priority queues.

Packets are transmitted according to the following principles:

- Packets from the highest priority queue are transmitted first.
- If a queue is in strict priority mode, it is allowed to transmit until it has no more packets or until a higher priority queue has packets to send.
- If a queue is in WRR mode, it is allowed to transmit a number of packets that is proportional to its configurable weight value. The weight is expressed as a percentage of the total bandwidth for each port.

A combination of strict queue and WRR queues can be configured at a port.

Queue Configuration Recommendations

It is recommended that higher numbered queues be configured with higher priority, weight, and minimum-bandwidth settings.

The following are recommended scenarios for strict priority (SP) and WRR queues:

- **All eight queues in SP mode** (q8 > q7 > q6 > q5 > q4 > q3 > q2 > q1). q8 is allocated bandwidth as long as there are packets to serve in q8. Then Q7 is served, followed by Q6, and so forth.
- **All 8-queues in WRR mode** (q8:q7:q6:q5:q4:q3:q2:q1 = A:B:C:D:E:F:G:H). In this mode, each queue is allocated its minimum bandwidth according to the weights configured.
- **One queue in SP mode and all other queues in WRR mode** (q8 > q7/q6/.../q1 and q7::q1 = A::G). In this scenario q8 is configured in SP mode and q7 through q1 in WRR mode.
- **Four queues in SP mode and four queues in WRR mode** (q8 > q7 > q6 > q5 > q4/q3/q2/q1 and q4/q3/q2/q1 = A:B:C:D): In this scenario q8, q7, q6, and q5 are configured in strict mode with q4, q3, q2 and q1 in WRR mode.

When there are more ingress ports with traffic destined to different queues on egress ports, a system might encounter a Head of Line Blocking (HOL) condition. HOL could result in higher numbered queues getting more bandwidth, although higher numbered queues are configured with lower bandwidth and weight. It is always recommended that higher numbered queues with higher weight be configured in SP mode, so that even in a HOL condition, the desired egress segregation is achieved.

Configuring Queues

To configure QoS properties:

STEP 1 Click **Quality of Service** > **Queue** in the navigation window.

STEP 2 Select from the Interface drop-down menus the Port or the LAG to configure.

STEP 3 Select one of the following modes for each queue on the selected interface:

- **Strict Priority**—Select to have the scheduler forward traffic strictly based on the priority levels in the queues. The queue with the highest priority traffic has access to the egress port until all such traffic is forwarded. Strict priority mode provides low-latency service to higher priority classes of traffic.

- **WRR**—Select to have the scheduler service the queue in turn with other WRR queues, based on bandwidth percentage of the queue relative to other WRR queues. (Strict queues continue to be serviced for as long as they have higher priority traffic.)

STEP 4 If you selected WRR mode for a queue, enter a bandwidth percentage in the Percentage of WRR Bandwidth field. The total of all bandwidth percentages for all queues cannot exceed 100 percent.

STEP 5 Click **Apply**. Your changes are saved to the Running Configuration.

To apply these queue properties to all other interfaces on the switch, click **Copy Settings to All Interfaces**.

Mapping CoS/802.1p Priorities to Queues

The priority of a packet arriving on an interface might be identified by an IEEE 802.1p priority value in the Ethernet frame header. 802.1p specifies eight priority levels (0–7). Use the *CoS/802.1p to Queue* page to map these priority levels to the four CoS queues to *steer* packets to the appropriate outbound queue. Queue 1 has the lowest priority and queue 4 has the highest priority.

To map 802.1p priority values to queues:

STEP 1 Click **Quality of Service** > **CoS/802.1p to Queue** in the navigation window.

STEP 2 Select from the Interface drop-down menus the Port or the LAG to configure.

STEP 3 For each 802.1p Class of Service, select a queue from the Output Queue list. Queue 1 has the lowest priority, and queue 4 has the highest priority.

STEP 4 Click **Apply**. Your changes are saved to the Running Configuration.

STEP 5 To apply these mappings to all other interfaces on the switch, click **Copy Settings to All Interfaces**.

NOTE If you click **Restore Defaults**, the following mappings are applied to the selected interface.

802.1p Priority	Output Queue
0	1
1	1
2	2
3	3
4	3
5	4
6	4
7	4

Mapping IP Precedence to Queues

802.1p Priority	Output Queue
0	3
1	1
2	2
3	4
4	5
5	6
6	7
7	8

The priority of a packet arriving at an interface can be identified by the Type of Service (ToS) field in an IP packet header. Eight precedence levels are defined (0-7). You can use the *IP Precedence to Queue* page to map these values to the four. CoS queues to steer packets to the appropriate outbound queue. Queue 1 has the lowest priority and queue 4 has the highest priority.

NOTE IP Precedence-to-queue mapping is configured per interface. Configure these mapping values on the incoming interface.

To map IP precedence values to queues:

STEP 1 Click **Quality of Service** > **IP Precedence to Queue** in the navigation window.

STEP 2 Select from the Interface drop-down menus the Port or the LAG to configure.

STEP 3 For each IP Precedence value, select a queue from the Output Queue list. Queue 1 has the lowest priority, and queue 4 has the highest priority.

STEP 4 Click **Apply**. Your changes are saved to the Running Configuration.

To apply these mappings to all other interfaces on the switch, click **Copy Settings to All Interfaces**.

NOTE If you click **Restore Defaults**, the following mappings are applied to all interfaces.

IP Precedence	Output Queue
0	1
1	1
2	2
3	3
4	3
5	4
6	3
7	3

Mapping DSCP Values to Queues

The priority of a packet arriving at an interface can be identified by the Differentiated Service Code Point (DSCP) value in an IP packet header. The IP DSCP field might contain any one of 64 values (0–63). You can use the *DSCP to Queue* page to map these values to the four egress queues. Queue 1 has the lowest priority and queue 4 has the highest priority.

DSCP mapping settings are applied globally to all ports.

To map DSCP values to queues:

STEP 1 Click **Quality of Service** > **DSCP to Queue** in the navigation window.

STEP 2 For each Ingress DSCP value, select a queue from the Output Queue list. Queue 1 has the lowest priority, and queue 4 has the highest priority.

STEP 3 Click **Apply**. Your changes are saved to the Running Configuration.

NOTE If you click **Restore Defaults**, the following mappings are applied to all interfaces.

DSCP Value	Output Queue
00-07	1
08-15	1
16-23	2
24-31	3
32-39	3
40-47	4
48-55	3
56-63	3

Defining Rate Limit Profiles

The rate-limiting feature enables you to set a maximum incoming traffic rate for a port. When the data rate exceeds configured rate, the switch drops all further traffic from the port. Rate limits are applied per port.

To apply rate limits, you first use this page to create one or more rate limit profiles. Profiles specify the criteria that determines when the rate limit is exceeded. Then, you assign rate limit profiles to interfaces (see **Applying Rate Limit Profiles to Interfaces**).

To add an entry to the Rate limit Profile Table:

STEP 1 Click **Quality of Service** > **Rate Limit Profile** in the navigation window.

STEP 2 Click **Add**.

STEP 3 Enter the parameters:

- **Profile ID**—Specify any number from 1 to 64 to identify the profile.
- **CIR**—Specify the committed information rate, which is the rate at which data is transmitted. The rate is averaged over a minimum time increment. The range is 64-1048576 Kbps.

- **CBS**—Specify a committed burst size, which is the guaranteed amount of bandwidth for bursty traffic on the port. The range is 4-16384 KB.

STEP 4 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Applying Rate Limit Profiles to Interfaces

If you have created one or more rate limit profiles, you can use this page to assign them to interfaces. See **Defining Rate Limit Profiles** for instructions on creating profiles.

To apply a rate limit profile to an interface.

STEP 1 Click **Quality of Service** > **Interface Rate Limit** in the navigation window.

STEP 2 Use the Interface Type list to display Ports or LAGs in the Interface Rate Limit Table.

STEP 3 Select the interface to configure and click **Edit**.

STEP 4 Add or remove a profile:

- To assign a profile to this interface, click the profile ID in the Available list, and then click the right-arrow button to move it to the Selected list. All profiles disappear from the Available list, since only one profile can be assigned to a port.
- To remove a profile, click the profile ID in the Selected list, and then click the left-arrow button to move it to the Available list. All profiles appear in the Selected list.

STEP 5 Click **Apply** and then click **Close**. Your changes are saved to the Running Configuration.

Traffic Shaping

You can use the *Traffic Shaping* page to smooth the packet output rate. You can configure the maximum output rate for each port and LAG, expressed as a percentage of bandwidth. When the traffic rate reaches this limit, excess packets are retained in a queue and then are scheduled for later transmission over increments of time.

To configure traffic shaping on a port or LAG:

STEP 1 Click **Quality of Service** > **Traffic Shaping** in the navigation window.

STEP 2 Use the Interface Type menu to display Ports or LAGs in the Traffic Shaping Settings table.

STEP 3 Select the interface to configure and click **Edit**.

STEP 4 For the selected Port or LAG, enter the output rate limit as a percentage of the total bandwidth and click **Apply**.

STEP 5 Repeat the previous step as needed to assign bandwidth utilization to other ports and LAGs.

STEP 6 When you are finished, click **Close**. Your changes are saved to the Running Configuration.

78-19562-01