



ADMINISTRATION GUIDE

Cisco Small Business 200 Series Smart Switch Administration Guide Release 1.1

10/100 Switches
Gigabit Switches

SF200-24, SF200-24P, SF200-48, SF200-48P
SG200-18, SG200-26, SG200-26P, SG200-50, SG200-50P

Chapter 1: Getting Started	1
Starting the Web-based Switch Configuration Utility	1
Launching the Configuration Utility	1
Logging In	2
Password Expiration	5
Logging Out	5
Quick Start Switch Configuration	6
Window Navigation	7
Application Header	7
Management Buttons	9
Chapter 2: Viewing Statistics	12
Viewing Ethernet Interface	12
Viewing Etherlike Statistics	15
Viewing 802.1X EAP Statistics	17
Managing RMON Statistics	18
Viewing RMON Statistics	19
Configuring RMON History	21
Viewing the RMON History Table	23
Defining RMON Events Control	25
Viewing the RMON Events Logs	27
Defining RMON Alarms	28
Chapter 3: Managing System Logs	31
Setting System Log Settings	31
Setting Remote Logging Settings	34
Viewing Memory Logs	36
RAM Memory	36
Flash Memory	38

Chapter 4: Managing System Files	39
Upgrade/Backup Firmware/Language	42
Downloading or Backing-up a Configuration or Log	45
Displaying Configuration File Properties	49
Copying Configuration Files	50
Setting DHCP Auto Configuration	52
Chapter 5: System Time	55
System Time Options	56
Configuring System Time	57
Adding an SNTP Server	59
Defining SNTP Authentication	63
Chapter 6: General Administrative Information and Operations	66
System Information	67
Displaying the System Summary	67
Configuring the System Settings	69
Switch Models	70
Rebooting the Switch	71
Monitoring the Fan Status	73
Defining Idle Session Timeout	74
Pinging a Host	75
Chapter 7: Configuring Discovery	77
Configuring Bonjour Discovery	77
Configuring LLDP	78
Setting LLDP Properties	80
Editing LLDP Port Settings	81
LLDP MED Protocol	85
Setting LLDP MED Network Policy	85
Configuring LLDP MED Port Settings	88

Displaying LLDP Port Status	90
Displaying LLDP Local Information	92
Displaying LLDP Neighbors Information	96
Accessing LLDP Statistics	101
LLDP Overloading	102

Chapter 8: Port Management **106**

Configuring Ports	106
Port Management Workflow	106
Setting the Basic Port Configuration	107
Configuring Link Aggregation	111
Static and Dynamic LAG Workflow	112
Defining LAG Management	113
Defining Member Ports in a LAG	114
Configuring LAG Settings	115
Configuring LACP	117
Setting Port LACP Parameter Settings	118
Green Ethernet	120
Setting Global Green Ethernet Properties	121
Setting Green Ethernet Properties for Ports	123

Chapter 9: Managing Device Diagnostics **125**

Testing Copper Ports	125
Displaying Optical Module Status	129
Configuring Port and VLAN Mirroring	131
Viewing CPU Utilization	134

Chapter 10: Managing Power-over-Ethernet Devices **135**

PoE on the Switch	135
PoE Features	135
PoE Operation	136
PoE Configuration Considerations	136

Configuring PoE Properties	137
Configuring the PoE Power, Priority, and Class	139
Chapter 11: VLAN Management	143
VLANs	143
Configuring Default VLAN Settings	145
Creating VLANs	147
Configuring VLAN Interface Settings	150
Defining VLAN Membership	153
Configuring Port to VLAN	154
Configuring VLAN to Port	155
Viewing VLAN Membership	158
Voice VLAN	159
Voice VLAN Options	160
Configuring Voice VLAN Properties	161
Configuring Telephony OUI	163
Chapter 12: Configuring the Spanning Tree Protocol	165
STP Flavors	165
Configuring STP Status and Global Settings	166
Defining Spanning Tree Interface Settings	169
Configuring Rapid Spanning Tree Settings	172
Chapter 13: Managing MAC Address Tables	176
Configuring Static MAC Addresses	176
Dynamic MAC Addresses	178
Configuring Dynamic MAC Address Parameters	179
Querying Dynamic Addresses	179
Chapter 14: Configuring Multicast Forwarding	182
Multicast Forwarding	182

Typical Multicast Setup	183
Multicast Operation	183
Multicast Registration	184
Multicast Address Properties	185
Defining Multicast Properties	185
Adding MAC Group Address	188
Adding IP Multicast Group Address	192
Configuring IGMP Snooping	195
Configuring MLD Snooping	199
Viewing GMP/MLD IP Multicast Groups	202
Defining Multicast Router Ports	203
Defining Forward All Multicast	205
Defining Unregistered Multicast Settings	207

Chapter 15: Configuring IP Information 210

Management and IP Interfaces	210
IP Addressing	212
Defining an IPv4 Interface	213
Defining IPv6 Global Configuration	215
Defining an IPv6 Interface	216
Defining IPv6 Addresses	218
Viewing the IPv6 Default Router List	220
Configuring IPv6 Tunnels	223
Defining IPv6 Neighbors Information	225
Viewing IPv6 Route Tables	229
Configuring ARP	230
Domain Name Systems	233
Defining DNS Servers	233
Mapping DNS Hosts	235

Chapter 16: Configuring Security	238
Defining Users	240
Setting User Accounts	240
Setting Password Complexity Rules	242
Configuring RADIUS Parameters	244
Configuring Management Access Authentication	248
Defining Access Profiles	250
Displaying, Adding, or Activating an Access Profile	251
Defining Profile Rules	254
Configuring TCP/UDP Services	257
Defining Storm Control	259
Configuring Port Security	262
Configuring 802.1X	265
802.1X Parameters Workflow	266
Defining 802.1X Properties	267
Defining 802.1X Port Authentication	268
Defining Host and Session Authentication	271
Viewing Authenticated Hosts	274
Chapter 17: Configuring Quality of Service	275
QoS Features and Components	275
Configuring QoS	277
Displaying QoS Properties	277
Defining QoS InterfaceSettings	279
Configuring QoS Queues	281
Mapping CoS/802.1p to a Queue	283
Mapping DSCP to Queue	285
Configuring Bandwidth	286
Configuring Egress Shaping per Queue	288
Managing QoS Statistics	290
Viewing Queues Statistics	290

Getting Started

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

- [Starting the Web-based Switch Configuration Utility](#)
- [Quick Start Switch Configuration](#)
- [Window Navigation](#)

Starting the Web-based Switch Configuration Utility

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

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

Browser Restrictions

Browsers have the following restrictions:

- If you are using Internet Explorer 6, you cannot directly use an IPv6 address to access the switch. You can, however, use the DNS (Domain Name System) server to create a domain name that contains the IPv6 address, and then use that domain name in the address bar in place of the IPv6 address.
- In Firefox, the automatic pop-up on top option is disabled by default. Certain add-ons enable this feature during installation. To disable this option, go to `ToolsOptionsContentEnable JavaScriptAdvance`.
- If you have multiple IPv6 interfaces on your management station, use the IPv6 global address instead of IPv6 link local address to access the switch from your browser.

Launching the Configuration Utility

To open the user interface:

-
- STEP 1** Open a Web browser.
 - STEP 2** Enter the IP address of the switch you are configuring in the address bar on the browser, and then press **Enter**. The *Login* page opens.

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

Logging In

Logging In

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

To log in to the device configuration utility:

-
- STEP 1** Enter the username/password. The password can contain up to 64 ASCII characters. Password-complexity rules are described in the **Setting Password Complexity Rules** section of the **Configuring Security** chapter.
 - STEP 2** If you are not using English, select the desired language from the *Language* drop-down menu. To add a new language to the switch or update a current one, refer to the *Upgrade/Backup Firmware/Language* section.
 - STEP 3** If this is the first time that you logged on with the default user ID (**cisco**) and the default password (**cisco**) or your password has expired, the *Change Password* Page opens. See *Password Expiration* for additional information.
 - STEP 4** Choose whether to select **Disable Password Complexity Enforcement** or not. For more information on password complexity, see the *Setting Password Complexity Rules* section.
 - STEP 5** Enter the new password and click **Apply**.

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

If you entered an incorrect username or password, an error message is displayed and the *Login* page remains displayed on the window. If you are having problems logging in, please see the [Launching the Configuration Utility](#) section in the Administration Guide for additional information.

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

Password Expiration

Password Expiration

The *New Password* page is displayed:

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

Logging Out

Logging Out

By default, the application logs out after ten minutes of inactivity. You can change this default value as described in the [Defining Idle Session Timeout](#) section in the [General Administrative Information and Operations](#) chapter.



CAUTION

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

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

When the switch auto-discovers a device, such as an IP phone, it configures the

port appropriately for the device. These configuration commands are written to the Running Configuration file. This causes the Save icon to begin blinking when the user logs on even though the user did not make any configuration changes.

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

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

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

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

Quick Start Switch Configuration

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

Links on the Getting Started page

Category	Link Name (on the Page)	Linked Page
Initial Setup	Change Device IP Address	<i>IPv4 Interface</i> page
	Create VLAN	<i>Create VLAN</i> page
	Configure Port Settings	<i>Port Setting</i> page
Device Status	System Summary	<i>System Summary</i> page
	Port Statistics	<i>interface</i> page
	RMON Statistics	<i>Statistics</i> page

Links on the Getting Started page (Continued)

Category	Link Name (on the Page)	Linked Page
	View Log	<i>RAM Memory</i> page
Quick Access	Change Device Password	<i>User Accounts</i> page
	Upgrade Device Software	<i>Upgrade/Backup Firmware/ Language</i> page
	Backup Device Configuration	<i>Download/Backup Configuration/Log</i> page
	Configure QoS	<i>QoS Properties</i> page
	Configure Port Mirroring	<i>Port and VLAN Mirroring</i> page

There are two hot links on the Getting Started page that take you to Cisco web pages for more information. Clicking on the **Support** link takes you to the switch product support page, and clicking on the **Forums** link takes you to the Small Business Support Community page.

Window Navigation


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

Application Header


Application Header

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

Application Links

Application Link Name	Description
	<p>A flashing red X icon displayed to the left of the Save application link indicates that Running Configuration changes have been made that have not yet been saved to the Startup Configuration file. The flashing of the red X can be disabled on the Copy/Save Configuration page.</p> <p>Click Save to display the <i>Copy/Save Configuration</i> page. Save the Running Configuration file type by copying it to the Startup Configuration file type on the switch. After this save, the red X icon and the Save application link are no longer displayed. When the switch is rebooted, it copies the Startup Configuration file type to the Running Configuration and sets the switch parameters according to the data in the Running Configuration.</p>
Username	Displays the name of the user logged on to the switch. The default username is cisco . (The default password is cisco .)
Language Menu	Select a language or load a new language file into the switch. If the language required is displayed in the menu, select it. If it is not displayed, select Download Language . For more information about adding a new language, refer to the <i>Upgrade/Backup Firmware/Language</i> .
Logout	Click to logout of the web-based switch configuration utility.

Application Links (Continued)

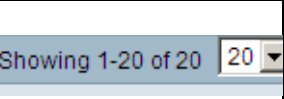

Application Link Name	Description
About	Click to display the switch name and switch version number.
Help	Click to display the online help.
	The SYSLOG Alert Status icon is displayed when a SYSLOG message, above the <i>critical</i> severity level, is logged. Click the icon to open the <i>RAM Memory</i> page. After you access this page, the SYSLOG Alert Status icon is no longer displayed. To display the page when there is not an active SYSLOG message, follow the Status and Statistics > View Log > RAM Memory page path.

Management Buttons

Management Buttons

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

Management Buttons

Button Name	Description
	The Administrator can use the pull-down menu to configure how many entries per page they wish to see at a time.
	Indicates a mandatory field.
Add	Click to display the related <i>Add</i> page and add an entry to a table. Enter the information and click Apply to save it to the Running Configuration. Click Close to return to the main page. Click Save to display the <i>Copy/Save Configuration</i> page and save the Running Configuration to the Startup Configuration file type on the switch.

Management Buttons (Continued)

Button Name	Description
Apply	Click to apply changes to the Running Configuration on the switch. If the switch is rebooted, the Running Configuration is lost, unless it is saved to the Startup Configuration file type or another file type. Click Save to display the <i>Copy/Save Configuration</i> page and save the Running Configuration to the Startup Configuration file type on the switch.
Cancel	Click to reset changes made on the page.
Clear All Interfaces Counters	Click to clear the statistic counters for all interfaces.
Clear Interface Counters	Click to clear the statistic counters for the selected interface.
Clear Logs	Clears log files.
Clear Table	Clears table entries.
Close	Returns to main page. If there are changes that were not applied to the Running Configuration, a message is displayed.
Copy Settings	<p>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:</p> <ol style="list-style-type: none"> 1. Select the entry to be copied. Click Copy Settings to display the popup. 2. Enter the destination entry numbers in the to field. 3. Click Apply to save the changes and click Close to return to the main page.
Delete	Select the entry in the table to be deleted and click Delete to remove entries from a table. The entry is deleted.
Details	Click to display the details associated with the entry selected on the main page.

Management Buttons (Continued)

Button Name	Description
Edit	Select the entry and click Edit to open the entries for editing. The <i>Edit</i> page opens, and the entry can be modified. <ol style="list-style-type: none">1. Click Apply to save the changes to the Running Configuration.2. Click Close to return to the main page.
Go	Enter the query filtering criteria and click Go . The results are displayed on the page.
Test	Click Test to perform the related tests.

Viewing Statistics

This section describes how to view switch statistics.

It contains the following sections:

- [Viewing Ethernet Interface](#)
- [Viewing Etherlike Statistics](#)
- [Viewing 802.1X EAP Statistics](#)
- [Managing RMON](#)

Viewing Ethernet Interface

The *Interface* page displays traffic statistics per port. The refresh rate of the information can be selected.

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

To display Ethernet statistics:

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

STEP 2 Enter the parameters.

- **Interface**—Select the type of interface and specific interface for which Ethernet statistics are to be displayed.
- **Refresh Rate**—Select the time period that passes before the interface Ethernet statistics are refreshed. The available options are:
 - *No Refresh*—Statistics are not refreshed.
 - *15 Sec*—Statistics are refreshed every 15 seconds.
 - *30 Sec*—Statistics are refreshed every 30 seconds.

- 60 Sec—Statistics are refreshed every 60 seconds.

The Receive Statistics area displays information about incoming packets.

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

The Transmit Statistics area displays information about outgoing packets.

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

To clear statistics counters:

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

Viewing Etherlike Statistics

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

To view Etherlike Statistics:

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

STEP 2 Enter the parameters.

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

The fields are displayed for the selected interface.

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

To clear statistics counters:

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

Viewing 802.1X EAP Statistics

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

To view the EAP Statistics:

-
- STEP 1** Click **Status and Statistics** > **802.1X EAP**. The *802.1x EAP* page opens.
 - STEP 2** Select the **Port** that is polled for statistics.
 - STEP 3** Select the time period (**Refresh Rate**) that passes before the EAP statistics are refreshed.

The values are displayed for the selected interface.

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

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

To clear the counters for a specified interface, click **Clear Interface Counters**. To clear the counters for all interfaces, click **Clear All Interface Counters**.

Managing RMON

RMON (Remote Networking Monitoring) enables the switch to proactively monitor traffic statistics over a given period.

With this feature, you can view statistics (counter values) as they are currently, meaning since the last time they were cleared.

Viewing RMON Statistics

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

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

To view the RMON statistics:

- STEP 1** Click **RMON > Statistics**. The *Statistics* page opens.
- STEP 2** Select the **Interface** for which Ethernet statistics are to be displayed.
- STEP 3** Select the **Refresh Rate**, the time period that passes before the interface statistics are refreshed.

The statistics are displayed for the selected interface.

- **Bytes Received (Octets)**—Number of octets received, including bad packets and FCS octets, but excluding framing bits.
- **Drop Events**—Number of packets that were dropped.
- **Packets Received**—Number of good packets received, including Multicast and Broadcast packets.
- **Broadcast Packets Received**—Number of good Broadcast packets received. This number does not include Multicast packets.
- **Multicast Packets Received**—Number of good Multicast packets received.
- **CRC & Align Errors**—Number of CRC and Align errors that have occurred.
- **Undersize Packets**—Number of undersized packets (less than 64 octets) received.
- **Oversize Packets**—Number of oversized packets (over 1518 octets) received.
- **Fragments**—Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.
- **Jabbers**—Total number received packets that were longer than 1632 octets. This number excludes frame bits, but includes FCS octets that had either a bad FCS (Frame Check Sequence) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. A Jabber packet is defined as an Ethernet frame that satisfies the following criteria:
 - Packet data length is greater than MRU
 - Packet has an invalid CRC
 - Rx Error Event has not been detected
- **Collisions**—Number of collisions received. If Jumbo Frames are enabled, the threshold of Jabber Frames is raised to the maximum size of Jumbo Frames.
- **Frames of 64 Bytes**—Number of frames, containing 64 bytes that were received.
- **Frames of 65 to 127 Bytes**—Number of frames, containing 65-127 bytes that were received.

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

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

To reset the counters, click **Clear Interface Counters**, or **Clear All Interfaces Counters**

Managing System Logs

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

The switch generates the following local logs:

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

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

This section contains the following sections:

- [Setting System Log Settings](#)
- [Setting Remote Logging Settings](#)
- [Viewing Memory Logs](#)

Setting System Log Settings

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

Severity Levels

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

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

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

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

Selecting a severity level to be stored in a log causes all of the higher severity events to be automatically stored in the log. Lower severity events are not stored in the log.

For example, if **Warning** is selected, all severity levels that are **Warning** and higher are stored in the log (Emergency, Alert, Critical, Error, and Warning). No events with severity level below **Warning** are stored (Notice, Informational, and Debug).

To set global log parameters:

-
- STEP 1** Click **Administration > System Log > Logs Settings**. The *Log Settings* page opens.
- STEP 2** Enter the parameters.
- **Logging**—Select to enable message logging.
 - **Syslog Aggregation**—Select to enable the aggregation of SYSLOG messages and traps. If enabled, identical and contiguous SYSLOG messages and traps are aggregated over an interval of time and sent in a single message. The aggregated messages are sent in the order of their arrival. Each message states the number of times it has been aggregated.
 - **Max Aggregation Time**—Enter the interval of time that SYSLOG messages are aggregated.

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

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

Setting Remote Logging Settings

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

To define SYSLOG servers:

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

This page displays the list of remote log servers.

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

STEP 3 Enter the parameters.

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

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

STEP 4 Click **Apply**. The *Add Remote Log Server* page closes, the SYSLOG server is added, and the Running Configuration file is updated.

Viewing Memory Logs

The switch can write to the following logs:

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

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

RAM Memory

RAM Memory

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

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

The top of the page has a button that allows you to Disable Alert Icon Blinking. Click to toggle between disable and enable.

This page displays the following fields:

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

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

Flash Memory

Flash Memory

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

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

This page displays the following fields:

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

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

Managing System Files

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

The methods of file transfer are:

- Internal copy.
- HTTP that uses the facilities that the browser provides.
- TFTP client, requiring a TFTP server.

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

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

Files and File Types

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

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

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

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

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

The Startup Configuration is retained in Flash and is preserved any time the switch is rebooted. When it is rebooted, the Startup Configuration is copied to RAM and identified as the Running Configuration.

- **Backup Configuration**—A manual copy of the parameter definitions for protection against system shutdown or for the maintenance of a specific operating state. You can copy the Mirror Configuration, Startup Configuration, or Running Configuration to a Backup Configuration file. The Backup Configuration exists in Flash and is preserved if the device is rebooted.
- **Mirror Configuration**—A copy of the Startup Configuration, created by the switch after:
 - The switch has been operating continuously for 24 hours.
 - No configuration changes have been made to the Running Configuration in the previous 24 hours.
 - The Startup Configuration is identical to the Running configuration.

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

If the switch is rebooted, the Mirror Configuration is reset to the factory default parameters. In all other aspects, the Mirror Configuration behaves the same as a Backup Configuration, providing a copy of the parameter values that is preserved if the switch is rebooted.

- **Firmware**—The program that controls the operations and functionality of the switch. More commonly referred to as the *image*.
- **Boot Code**—Controls the basic system startup and launches the firmware image.

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

File Actions

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

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



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

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

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

This section describes how configuration and log files are managed.

It includes the following topics:

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

Upgrade/Backup Firmware/Language

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

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

The following methods for transferring files are supported:

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

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

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

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

Uploading a New Firmware or Language File

To download or backup a system or language file:

- STEP 1** Click **Administration > File Management > Upgrade/Backup Firmware/Language**. The *Upgrade/Backup Firmware/Language* page opens.
- STEP 2** Click the Transfer Method. If you selected TFTP, go to **STEP 3**. If you selected HTTP, go to **STEP 4**.
- STEP 3** If you selected TFTP, enter the parameters as described in this step. Otherwise, skip to **STEP 4**.

Select either the Upgrade or Backup **Save Action**.

Upgrade Save Action—Specifies that the file type on the switch is to be replaced with a new version of that file type located on a TFTP server. Enter the following fields.

- a. **File Type**—Select the destination file type. Only valid file types are shown. (The file types are described in the **Files and File Types** section.) Note that the boot code can only be upgraded via TFTP.
- b. **Server Definition**—Select whether to specify the TFTP server by IP address or domain name.
- c. **IP Version**—Select whether an IPv4 or an IPv6 address is used.
- d. **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are:

Link Local—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.

Global—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.

- e. **Link Local Interface**—Select the link local interface (if IPv6 is used) from the list.
- f. **TFTP Server IP Address/Name**—Enter the IP address or the domain name of the TFTP server.
- g. **Source File Name**—Enter the name of the source file.

Backup Save Action—Specifies that a copy of the file type is to be saved to a file on another device. Enter the following fields:

- a. **File Type**—Select the source file type. Only valid file types can be selected. (The file types are described in the **Files and File Types** section.)
- b. **Server Definition**—Select either By IP Address or By name.
- c. **IP Version**—Select whether an IPv4 or an IPv6 address is used.
- d. **IPv6 Address Type**—Select the IPv6 address type (if used). The options are:
 - Link Local**—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of FE80, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
 - Global**—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- e. **Link-Local Interface**—Select the link local interface (if IPv6 is used) from the list.
- f. **TFTP Server IP Address/Name**—Enter the IP address of the TFTP server.
- g. **Destination File Name**—Enter the destination file name. File names cannot contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the file name should be between 1 and 160 characters. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”).

STEP 4 If you selected **HTTP**, you can only Upgrade. Enter the parameters as described in this step.

- a. **File Type**—Select the configuration file type. Only valid file types can be selected. (The file types are described in the **Files and File Types** section.)
- b. **File Name**—Click **Browse** to select a file or enter the path and source file name to be used in the transfer.

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

Language Files

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

-
- STEP 1** Click **Delete Language**.
 - STEP 2** A confirmation window appears asking you to click **OK** to remove the file.
 - STEP 3** Click **OK** to remove the file.
-

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

Downloading or Backing-up a Configuration or Log

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

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

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

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

To backup or restore the system configuration file:

-
- STEP 1** Click **Administration > File Management > Download/Backup Configuration/Log**. The *Download/Backup Configuration/Log* page opens.
 - STEP 2** Click the Transfer Method.
 - STEP 3** If you selected TFTP, enter the parameters. Otherwise, skip to **STEP 4**.

Select either Download or Backup as the **Save Action**.

Download Save Action—Specifies that the file on another device will replace a file type on the switch. Enter the following fields:

- a. **Server Definition**—Select whether to specify the TFTP server by IP address or by domain name.
- b. **IP Version**—Select whether an IPv4 or an IPv6 address is used.

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

- c. **IPv6 Address Type**—Select the IPv6 address type (if used). The options are:
 - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
 - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- d. **Link-Local Interface**—Select the link local interface from the list.
- e. **TFTP Server**—Enter the IP address of the TFTP server.
- f. **Source File Name**—Enter the source file name. File names cannot contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the file name should be between 1 and 160 characters. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”).
- g. **Destination File Type**—Enter the destination configuration file type. Only valid file types are displayed. (The file types are described in the **Files and File Types** section.)

Backup Save Action—Specifies that a file type is to be copied to a file on another device. Enter the following fields:

- a. **Server Definition**—Select whether to specify the TFTP server by IP address or by domain name.
- a. **IP Version**—Select whether an IPv4 or an IPv6 address is used.
- b. **IPv6 Address Type**—Select the IPv6 address type (if used). The options are:
 - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
 - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- c. **Link-Local Interface**—Select the link local interface from the list.
- d. **TFTP Server IP Address/Name**—Enter the IP address or domain name of the TFTP server.
- e. **Source File Type**—Enter the source configuration file type. Only valid file types are displayed. (The file types are described in the **Files and File Types** section.)
- f. **Destination File Name**—Enter the destination file name. File names cannot contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the file name should be between 1 and 160 characters. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”).

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

Select the **Save Action**.

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

- a. **Source File Name**—Click **Browse** to select a file or enter the path and source file name to be used in the transfer.
- b. **Destination File Type**—Select the configuration file type. Only valid file types are displayed. (The file types are described in the **Files and File Types** section.)
- c. Click **Apply**. The file is transferred from the other device to the switch.

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

- a. **Source File Type**—Select the configuration file type. Only valid file types are displayed. (The file types are described in the **Files and File Types** section.)
- b. Click **Apply**. The **Download/Backup Configuration/Log** window displays.

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

Displaying Configuration File Properties

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

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

This page provides the following fields:

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

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

Copying Configuration Files

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

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



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

The following combinations of copying internal file types are allowed:

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

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

-
- STEP 1** Click **Administration > File Management > Copy/Save Configuration**. The *Copy/Save Configuration* page opens.
- STEP 2** Select the **Source File Name** to be copied. Only valid file types are displayed. (The file types are described in the [Files and File Types](#) section.)
- STEP 3** Select the **Destination File Name** to be overwritten by the source file.
- STEP 4** Click **Apply**. The file is copied.
-

Setting DHCP Auto Configuration

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

DHCP Auto Configuration

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

NOTE If you enable DHCP Auto Configuration on a switch with DHCP disabled, you must enable the DHCP by using the procedure is described in the [Management and IP Interfaces](#) section.

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

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

- A configuration file that is placed on the TFTP server must match the form and format requirements of a supported configuration file. The form and format of the file are checked, but the validity of the configuration *parameters* is not checked prior to loading it to the Startup Configuration.
- To make sure the configuration of devices functions as intended and due to allocation of different IP addresses with each DHCP renew cycle, IP addresses must be bound to MAC addresses in the DHCP server table. This ensures that each device has its own reserved IP address and other relevant information.

To configure DHCP server auto configuration:

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

STEP 2 Enter the values.

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

The window displays the following:

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

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

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

System Time

Network time synchronization is critical because every aspect of managing, securing, planning, and debugging a network involves determining when events occur. Time provides a frame of reference between all devices on the network.

Without synchronized time, accurately correlating log files between devices, for instance when tracking security breaches or network usage, is not possible. Problems affecting a large number of components can be nearly impossible to track if timestamps in logs are inaccurate.

Time also reduces confusion in shared file systems, as it is important for the modification times to be consistent, regardless of the machine on which the files systems reside.

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

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

This section describes the options for configuring system time, time zone, and Daylight Savings Time (DST). It includes the following topics:

- [System Time Options](#)
- [Configuring System Time](#)
- [Adding an SNTP Server](#)
- [Defining SNTP Authentication](#)

System Time Options

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

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

Time

Time

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

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

NOTE This method is recommended for the sake of accuracy.

- **Manual**—The user can manually set the time.
- **From Browser**—Time can be received from the time of the PC using browser information. If this feature is enabled, the switch uses the system time from the configuring computer, unless the time has been configured on the switch manually by the user or SNTP server support is not available or enabled.

After the time has been set by any of the three time sources, it is not set again by the browser.

The configuration of time from browser is saved to the Running Configuration file. You must copy the Running Configuration to the Startup Configuration in order to enable the device to use the time from browser after reboot. The time after reboot is set during the first WEB login to the device.

When the user applies this feature for the first time, if the time was not already set, the device sets the time from the browser.

The time from browser works with both HTTP and HTTPS connections.

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

Time Zone and Daylight Savings Time (DST)

Time Zone and Daylight Savings Time (DST)

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

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

Configuring System Time

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



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

To define system time:

- STEP 1** Click **Administration > Time Settings > System Time**. The *System Time* page opens.
- STEP 2** Enter the parameters.

Clock Source Settings—Select the source used to set the system clock.

- **Main Clock Source (SNTP Servers)**—The system time is obtained from an SNTP server. To use this feature, you must also add an SNTP server or enable SNTP Broadcast mode by using the *SNTP Settings* page. Optionally, enforce authentication of the SNTP sessions by using the *SNTP Authentication* page. This feature does not function when the switch is in layer 3 mode.
- **Alternate Clock Source (PC via active HTTP/HTTPS sessions)**—Select to set the date and time from the configuring computer using the HTTP protocol.

NOTE If Alternate Clock Source is selected, the time will be taken from the PC running the GUI. Each time you log into the GUI, the time is taken from your PC.

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

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

Time Zone Settings—The local time is used via DHCP or Time Zone offset.

- **Get time zone from DHCP**—Select to enable dynamic configuration of the time zone and the DST from the DHCP server. Whether one or both of these parameters can be configured depends on the information found in the DHCP packet. If this option is enabled, *you must also enable DHCP client on the switch*. To do this, set the **IP Address Type** to **Dynamic** in the *IPv4 Interface* page.
- **Time Zone Offset**—Select the difference in hours between *Greenwich Mean Time* (GMT) and the local time. For example, the Time Zone Offset for Paris is GMT + 1, while the Time Zone Offset for New York is GMT – 5.

Daylight Savings Settings—Select how DST is defined:

- **Daylight Savings**—Check to enable daylight Savings Time.
- **Time Zone Offset**—Enter the number of minutes offset from GMT ranging from 1—1440. The default is 60.
- **Daylight Savings Type**—Click one of the following:
 - *USA*—DST will be set according to the dates used in the USA

- *European*—DST will be set according to the dates used by the European Union and other countries that use this standard.
- *By Dates*—DST will be set manually, typically for a country other than the USA or a European country. Enter the following parameters:
- *Recurring*—DST occurs on the same date every year. Enter the following parameters:

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

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

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

- **From**—Date when DST begins each year.
 - *Day*—Day of the week on which DST begins every year.
 - *Week*—Week within the month from which DST begins every year.
 - *Month*—Month of the year in which DST begins every year.
 - *Time*—The time at which DST begins every year.
- **To**—Date when DST ends each year. For example, DST ends locally every fourth Friday in October at 5:00 am. The parameters are:
 - *Day*—Day of the week on which DST ends every year.
 - *Week*—Week within the month from which DST ends every year.
 - *Month*—Month of the year in which DST ends every year.
 - *Time*—The time at which DST ends every year.

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

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

Adding an SNTP Server

Up to eight SNTP servers can be configured. In addition to configuring SNTP server(s), enable this feature by using the *SNTP Settings* page.

NOTE To specify an SNTP server by name, you must first configure DNS server(s) on the switch (see the [Defining DNS Servers](#) section).

The switch supports the following modes:

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

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

To add an SNTP server:

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

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

- **SNTP Server**—SNTP server IP address. Up to eight SNTP servers can be defined. The preferred server, or hostname, is chosen according to its stratum level.
- **Poll Interval**—Displays whether polling is enabled or disabled.
- **Authentication Key ID**—Key Identification used to communicate between the SNTP server and switch.
- **Stratum Level**—Distance from the reference clock expressed as a numerical value. An SNTP server cannot be the primary server (stratum level 1) unless polling interval is enabled.
- **Status**—SNTP server status. The possible options are:
 - *Up*—SNTP server is currently operating normally.
 - *Down*—SNTP server is currently not available.
 - *Unknown*—SNTP server is currently being searched for by the switch.

- *In Process*—Occurs when the SNTP server has not fully trusted its own time server (i.e. when first booting up the NTP server).
- **Last Response**—Date and time of the last time a response was received from this SNTP server.
- **Offset**—The estimated offset of the server's clock relative to the local clock, in milliseconds. The host determines the value of this offset using the algorithm described in RFC 2030.
- **Delay**—The estimated round-trip delay of the server's clock relative to the local clock over the network path between them, in milliseconds. The host determines the value of this delay using the algorithm described in RFC 2030.
- **Last Synchronized Server**—Appears at the bottom of the other selections, and displays the address of the SNTP server from which time was last taken.

STEP 2 (Optional) Select **SNTP Broadcast Reception** > **Enable** to listen to SNTP Broadcast synchronization packets for system time information. The system will only display an SNTP server once a successful broadcast has been received. This feature is not functional when the switch is in layer 3 mode.

STEP 3 Click **Add** to display the *Add SNTP Server* page.

STEP 4 Enter the following parameters:

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

NOTE To specify a well-known SNTP server, the switch must be connected to the Internet and configured with a DNS server or configured so that a DNS server is identified by using DHCP. (See the [Defining DNS Servers](#) section.)

- **IP Version**—Select the version of the IP address: **Version 6** or **Version 4**.
- **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are
 - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
 - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.

- **Link Local Interface**—Select the link local interface (if IPv6 Address Type Link Local is selected) from the list.
- **SNTP Server IP Address**—Enter the SNTP server IP address. The format depends on which address type was selected.
- **SNTP Server**—Select the name of the SNTP server from a list of well-known SNTP servers. If **other** is chosen, enter name of SNTP server in the adjacent field.
- **Poll Interval**—Select to enable polling of the SNTP server for system time information. All SNTP servers that are registered for polling are polled, and the clock is selected from the server with the lowest stratum level (distance from the reference clock.) that is reachable. The server with the lowest stratum is considered to be the primary server. The server with the next lowest stratum is a secondary server, and so forth. If the primary server is down, the switch polls all servers with the polling setting enabled, and selects a new primary server with the lowest stratum.
- **Authentication**—Select the check box to enable authentication.
- **Authentication Key ID**—If authentication is enabled, select the value of the key ID. (Create the authentication keys using the *SNTP Authentication* page.)

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

Defining SNTP Authentication

The *SNTP Authentication* page enables configuration of the authentication keys that are used when communicating with an SNTP server that requires authentication. The authentication key is created on the SNTP server in a separate process that depends on the type of SNTP server you are using. Consult with the SNTP server system administrator for more detail on this.

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

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

To define SNTP authentication:

-
- STEP 1** Click **Administration > Time Settings > SNTP Authentication**. The *SNTP Authentication* page opens.
- STEP 2** Select **SNTP Authentication** to require authentication of an SNTP session between the switch and an SNTP server.
- STEP 3** Click **Apply** to update the switch.
- STEP 4** Click **Add**. The *Add SNTP Authentication* page opens.
- STEP 5** Enter the following parameters:
- **Authentication Key ID**—Enter the number used to identify this SNTP authentication key internally.
 - **Authentication Key**—Enter the key used for authentication (up to eight characters). The SNTP server must send this key for the switch to synchronize to it.
 - **Trusted Key**—Select the check box to allow the switch to receive broadcast synchronization information only from a SNTP server by using this authentication key.
- STEP 6** Click **Apply**. The SNTP Authentication is defined, and the Running Configuration file is updated.
-

General Administrative Information and Operations

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

It includes the following topics:

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

System Information

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

Displaying the System Summary

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

The *System Summary* page displays system and hardware information.

System information:

- **System Description**—A description of the system.
- **System Location**—Physical location of the switch. Click **Edit** to go the *System Settings* page to enter this value.
- **System Contact**—Name of a contact person. Click **Edit** to go the *System Settings* page to enter this value.
- **Host Name**—Name of the switch. Click **Edit** to go the *System Settings* page to enter this value. By default, the switch hostname is composed of the word *switch* concatenated with the three least significant bytes of the switch MAC address (the six furthest right hexadecimal digits).
- **System Uptime**—Time that has elapsed since the last reboot.
- **Current Time**—Current system time.
- **Base MAC Address**—Switch MAC address.
- **Jumbo Frames**—Jumbo frame support status. This support can be enabled or disabled by using the *Port Setting* page.

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

TCP/UDP Services Status:

- **HTTP Service**—Displays whether HTTP is enabled/disabled.
- **HTTPS Service**—Displays whether HTTPS is enabled/disabled.
- **Edit**—Clicking on this takes you to *TCP/UDP Services* page. See *Configuring Security* for details.

Hardware and firmware version information:

- **Model Description**—Switch model description.
- **Serial Number**—Serial number.
- **PID VID**—Part number and version ID.
- **Firmware Version**—Firmware version number of the software image.
- **Firmware MD5 Checksum**—MD5 checksum of the software image.
- **Boot Version**—Boot version number.
- **Boot MD5 Checksum**—MD5 checksum of the boot version.

- **Locale**—Locale of the first language. (This is always English.)
- **Language Version**—Language package version of the first or English language.
- **Language MD5 Checksum**—MD5 checksum of the language file.
- **Locale**—Locale of the second language.
- **Language Version**—Language package version of the second language.
- **Language MD5 Checksum**—MD5 checksum of the secondary language file.

General PoE Status on models with PoE capability:

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

Configuring the System Settings

To enter system settings:

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

STEP 2 Modify the system settings.

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

- **Custom Login Screen Settings**—If you want text to be displayed on the *Login* page, enter the text in the **Login Banner** text box. Click **Preview** to view the results.

NOTE When the user defines a login banner from the web interface, it also activates the banner for the CLI interfaces (Console, Telnet, and SSH).

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

Switch Models

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

Layer 2 is the default mode of operation for all devices. In Layer 2 mode, the switch forwards packets as a VLAN aware bridge. In Layer 3 mode, the switch performs both IPv4 routing and VLAN aware bridging.

When the switch operates in Layer 3 mode, the VLAN Rate Limit, and QoS policers are not operational. Other QoS Advanced mode features are operational.

Fast Ethernet (10/100) ports are designated as **FE** and Gigabit Ethernet ports (10/100/1000) are designated as **GE** in the table below.

NOTE Acronyms used for port descriptions have varied across software versions. In release 1.0, 'e' was used for fast Ethernet, 'g' for 'gigabit Ethernet' in the GUI.

The following table describes the various models, the number and type of ports on them and the number of ports that support PoE.

Smart Switch Models

Model Name	Product ID (PID)	Description of Ports on Device	Power Dedicated to PoE	No. of Ports that Support PoE
SG200-18	SLM2016T	16 GE ports + 2 GE special-purpose combo ports		
SG200-26	SLM2024T	24 GE ports + 2 GE special-purpose combo-ports		

Smart Switch Models (Continued)

Model Name	Product ID (PID)	Description of Ports on Device	Power Dedicated to PoE	No. of Ports that Support PoE
SG200-26P	SLM2024PT	24 GE ports + 2 GE special-purpose combo-ports	100W	12 ports FE1-FE6, FE13 - FE18
SG200-50	SLM2048T	48 GE ports + 2 GE special-purpose combo-ports		
SG200-50P	SLM2048PT	48 GE ports + 2 GE special-purpose combo-ports	180W	24 ports FE1-FE12, FE25 - FE36
SF200-24	SLM224GT	24 FE ports + 2 GE special-purpose combo-ports		
SF200-24P	SLM224PT	24 FE ports + 2 GE special-purpose combo-ports	100W	12 ports FE1- FE6, FE13 - FE18
SF200-48	SLM248GT	48 FE ports + 2 GE special-purpose combo-ports		
SF200-48P	SLM248PT	FE1-FE48, GE1-GE4. 48 FE ports + 2 GE special-purpose combo-ports	180W	24 ports FE1- FE12, FE25 - FE36

Rebooting the Switch

Some configuration changes, such as enabling jumbo frame support, require the system to be rebooted before they take effect. However, rebooting the switch deletes the Running Configuration, so it is critical that the Running Configuration is saved to the Startup Configuration before the switch is rebooted. Clicking **Apply** does not save the configuration to the Startup Configuration. For more information on files and file types, see the [Files and File Types](#) section in the [Managing System Files](#) section.

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

To reboot the switch:

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

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

- **Reboot**—Reboots the switch. Since any unsaved information in the Running Configuration is discarded when the switch is rebooted, you must click **Save** in the upper-right corner of any window to preserve current configuration across the boot process. (If the Save option is not displayed, the Running Configuration matches the Startup Configuration and no action is necessary.)
- **Reboot to Factory Defaults**—Reboots the switch by using factory default configuration. This process erases the Startup Configuration file; any settings that are not saved to another file are cleared when this action is selected.



CAUTION DHCP Auto Configuration is enabled by default in the factory settings. In order to properly reboot the switch to factory defaults, you need to disable the DHCP Auto Configuration (for example connect the switch by local terminal and run the appropriate CLI to disable the auto configuration feature) so the switch does not automatically download a configuration from a local server.

Monitoring the Fan Status and Temperature

The *Health* page displays the switch fan status and temperature on the following devices:

SG200-50P

The page displays the fan status only on the rest of the devices.

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

The *Health* page displays the following fields:

- **Fan Status**—Fan status. OK indicates that the fans are operating normally.
 - **Temperature**—The internal temperature of the switch.
-

Defining Idle Session Timeout

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

- **HTTP Session Timeout**
- **HTTPS Session Timeout**

To set the idle session timeout of an HTTP or HTTPS session:

-
- STEP 1** Click **Administration** > **Idle Session Timeout**. The *Idle Session Timeout* page opens.
 - STEP 2** Select the timeout for the session from the corresponding list. The default timeouts are 10 minutes.
 - STEP 3** Click **Apply** to set the configuration settings on the switch.
-

Pinging a Host

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

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

To ping a host:

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

STEP 2 Configure ping by entering the fields:

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

-
- STEP 3** Click **Activate Ping** to ping the host. The ping status is displayed and another message is added to the list of messages, indicating the result of the ping operation.
- STEP 4** View the results of ping in the Ping Counters and Status section of the page.
-

Configuring Discovery

This section provides information for configuring Discovery.

It includes the following topics:

- [Configuring Bonjour Discovery](#)
- [LLDP and CDP](#)
- [Configuring LLDP](#)
- [Configuring CDP](#)

Configuring Bonjour Discovery

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

Bonjour for a System in Layer 2 Mode

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

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

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

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

To globally enable Bonjour:

- STEP 1** Click **Administration > Discovery - Bonjour**. The *Discovery - Bonjour* page opens.
- STEP 2** Select **Enable** to enable Bonjour Discovery globally on the switch.
- STEP 3** Click **Apply**. Bonjour is enabled or disabled on the switch according to the selection.

LLDP and CDP

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

The following are additional points about CDP/LLDP configuration:

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

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

NOTE CDP/LLDP does not distinguish if a port is in a LAG. If there are multiple ports in a LAG, CDP/LLDP transmit packets on each port without taking into account the fact that the ports are in a LAG.

The operation of CDP/LLDP is independent of the STP status of an interface.

If 802.1x port access control is enabled at an interface, the switch will transmit and receive CDP/LLDP packets to and from the interface only if the interface is authenticated and authorized.

If a port is the target of mirroring, then for CDP/LLDP it is considered down.

NOTE CDP and LLDP are link layer protocols for directly connected CDP/LLDP capable devices to advertise themselves and their capabilities. In deployments where the CDP/LLDP capable devices are not directly connected and are separated with CDP/LLDP incapable devices, the CDP/LLDP capable devices may be able to receive the advertisement from other device(s) only if the CDP/LLDP incapable devices flood the CDP/LLDP packets they receives. If the CDP/LLDP incapable devices perform VLAN-aware flooding, then CDP/LLDP capable devices can hear each other only if they are in the same VLAN. It should be noted that a CDP/LLDP capable device may receive advertisement from more than one device if the CDP/LLDP incapable devices flood the CDP/LLDP packets.

Configuring LLDP

This section describes how to configure LLDP. It contains the following topics:

- [LLDP Overview](#)
- [Setting LLDP Properties](#)
- [Editing LLDP Port Settings](#)
- [LLDP MED](#)
- [Configuring LLDP MED Port Settings](#)
- [Displaying LLDP Port Status](#)
- [Displaying LLDP Local Information](#)
- [Displaying LLDP Neighbors Information](#)
- [Accessing LLDP Statistics](#)
- [LLDP Overloading](#)

LLDP Overview

The Link Layer Discovery Protocol (LLDP) is a protocol that enables network managers to troubleshoot and enhance network management in multi-vendor environments. LLDP standardizes methods for network devices to advertise themselves to other systems, and to store discovered information.

LLDP enables a device to advertise its identification, configuration, and capabilities to neighboring devices that then store the data in a Management Information Base (MIB). The network management system models the topology of the network by querying these MIB databases.

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

The LLDP protocol has an extension called LLDP Media Endpoint Discovery (LLDP-MED), which provides and accepts information from media endpoint devices such as VoIP phones and video phones. For further information about LLDP-MED, see [LLDP MED](#).

LLDP Configuration Workflow

Following are examples of actions that can be performed with the LLDP feature and in a suggested order. You can refer to the LLDP/CDP section for additional guidelines on LLDP configuration. LLDP configuration pages are accessible under the **Administration > Discovery LLDP** menu.

1. Enter LLDP global parameters, such as the time interval for sending LLDP updates using the *LLDP Properties* page.
2. Configure LLDP per port by using the *Port Settings* page. On this page, interfaces can be configured to receive/transmit LLDP PDUs, send SNMP notifications, specify which TLVs to advertise, and advertise the switch's management address.
3. Create LLDP MED network policies by using the *LLDP MED Network Policy* page.
4. Associate LLDP MED network policies and the optional LLDP-MED TLVs to the desired interfaces by using the *LLDP MED Port Settings* page.
5. If Auto Smartport is to detect the capabilities of LLDP devices, enable LLDP in the Smartport Properties page.
6. Display overloading information by using the *LLDP Overloading* page.

Setting LLDP Properties

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

To enter LLDP properties:

-
- STEP 1** Click **Administration > Discovery - LLDP > Properties**. The *LLDP Properties* page opens.
- STEP 2** Enter the parameters.
- **LLDP Status**—Select to enable LLDP on the switch (selected by default).
 - **LLDP PDU Action**—If LLDP is not enabled, select the action to be taken if a packet that matches the selected criteria is received:
 - *Filtering*—Delete the packet.
 - *Flooding*—Forward the packet to all VLAN members.

- **TLV Advertise Interval**—Enter the rate in seconds at which LLDP advertisement updates are sent or use the default.
- **Topology Change System Log Notification Interval**—Enter the minimum time interval between system log notifications.
- **Hold Multiplier**—Enter the amount of time that LLDP packets are held before the packets are discarded, measured in multiples of the TLV Advertise Interval. For example, if the TLV Advertise Interval is 30 seconds, and the Hold Multiplier is 4, then the LLDP packets are discarded after 120 seconds.
- **Reinitializing Delay**—Enter the time interval in seconds that passes between disabling and reinitializing LLDP, following an LLDP enable/disable cycle.
- **Transmit Delay**—Enter the amount of time in seconds that passes between successive LLDP frame transmissions due to changes in the LLDP local systems MIB.

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

- STEP 3** In the **Fast Start Repeat Count** field, enter the number of times LLDP packets are sent when the LLDP-MED Fast Start mechanism is initialized. This occurs when a new endpoint device links to the switch.
- STEP 4** Click **Apply**. The LLDP properties are added to the Running Configuration file.

Editing LLDP Port Settings

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

The LLDP-MED TLVs to be advertised can be selected in the *LLDP MED Port Settings* page, and the management address TLV of the switch may be configured.

To define the LLDP port settings:

- STEP 1** Click **Administration > Discovery - LLDP > Port Settings**. The *Port Settings* page opens.
- This page displays the port LLDP information.
- STEP 2** Select a port and click **Edit**. The *Edit LLDP Port Settings* page opens.

This page provides the following fields:

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

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

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

- **Available Optional TLVs**—Select the information to be published by the switch by moving the TLV to the **Selected Optional TLVs** list. The available TLVs contain the following information:
 - *Port Description*—Information about the port, including manufacturer, product name and hardware/software version.
 - *System Name*—System's assigned name (in alpha-numeric format). The value equals the sysName object.
 - *System Description*—Description of the network entity (in alpha-numeric format). This includes the system's name and versions of the hardware, operating system, and networking software supported by the switch. The value equals the sysDescr object.
 - *System Capabilities*—Primary functions of the switch, and whether or not these functions are enabled in the switch. The capabilities are indicated by two octets. Bits 0 through 7 indicate Other, Repeater, Bridge, WLAN AP, Router, Telephone, DOCSIS cable device, and station respectively. Bits 8 through 15 are reserved.
 - *802.3 MAC-PHY*—Duplex and bit rate capability and the current duplex and bit rate settings of the sending device. It also indicates whether the current settings are due to auto-negotiation or manual configuration.

- *802.3 Link Aggregation*—Whether the link (associated with the port on which the LLDP PDU is transmitted) can be aggregated. It also indicates whether the link is currently aggregated, and if so, provides the aggregated port identifier.
- *802.3 Maximum Frame*—Maximum frame size capability of the MAC/PHY implementation.

The following fields relate to the Management Address:

- **Advertisement Mode**—Select one of the following ways to advertise the IP management address of the switch:
 - *Auto Advertise*—Specifies that the software would automatically choose a management address to advertise from all the IP addresses of the product. In case of multiple IP addresses the software chooses the lowest IP address among the dynamic IP addresses. If there are no dynamic addresses, the software chooses the lowest IP address among the static IP addresses.
 - *None*—Do not advertise the management IP address.
 - *Manual Advertise*—Select this option and the management IP address to be advertised.
- **IP Address**—If Manual Advertise was selected, select the Management IP address from the addresses provided.

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

LLDP MED

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

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

- Troubleshooting information. LLDP MED sends alerts to network managers upon:
 - Port speed and duplex mode conflicts
 - QoS policy misconfigurations

Setting LLDP MED Network Policy

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

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

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

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

To define an LLDP MED network policy:

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

This page displays previously-created network policies.

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

NOTE When this box is checked, the user may not manually configure a voice network policy.

- STEP 3** Click **Apply** to add this to the Running Configuration file.

- STEP 4** To define a new policy, click **Add** and the *Add LLDP MED Network Policy* page opens.
- STEP 5** Enter the values.
- **Network Policy Number**—Select the number of the policy to be created.
 - **Application**—Select the type of application (type of traffic) for which the network policy is being defined:
 - **VLAN ID**—Enter the VLAN ID to which the traffic should be sent.
 - **VLAN Tag**—Select whether the traffic is Tagged or Untagged.
 - **User Priority**—Select the traffic priority applied to traffic defined by this network policy. This is the CoS value.
 - **DSCP Value**—Select the DSCP value to associate with application data sent by neighbors. This informs them how they should mark the application traffic they send to the switch.
- STEP 6** Click **Apply**. The network policy is defined.

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

Configuring LLDP MED Port Settings

The LLDP MED Port Settings page enables the selection of the LLDP-MED TLVs and/or the network policies to be included in the outgoing LLDP advertisement for the desired interfaces. Network Policies are configured using the LLDP MED Network Policy page.

NOTE If LLDP-MED Network Policy for Voice Application (LLDP-MED Network Policy Page) is Auto and Auto Voice VLAN is in operation, then the switch will automatically generate an LLDP-MED Network Policy for Voice Application for all the ports that are LLDP-MED enabled and are members of the voice VLAN.

To configure LLDP MED on each port:

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

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

STEP 2 The message at the top of the page indicates whether the generation of the LLDP MED Network Policy for the voice application is automatic or not (see [LLDP Overview](#)). Click on the link to change the mode.

STEP 3 To associate additional LLDP MED TLV and/or one or more user-defined LLDP MED Network Policies to a port, select it, and click **Edit**. The *Edit LLDP MED Port Settings* page opens.

STEP 4 Enter the parameters.

- **Interface**—Select the interface to configure.
- **LLDP MED Status**—Enable/disable LLDP MED on this port.
- **System Log Notification**—Select whether the log notification is sent on a per-port basis, when an end station that supports MED has been discovered.
- **Available Optional TLVs**—Select the TLVs that can be published by the switch by moving them to the *Selected Optional TLVs* list.
- **Available Network Policies**—Select the LLDP MED policies that will be published by LLDP by moving them to the *Selected Network Policies* list. These were created in the *LLDP MED Network Policy* page. To include one or more user defined network polices in the advertisement, you must also select *Network Policy* from the *Available Optional TLVs*.

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

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

-
- STEP 5** Click **Apply**. The LLDP MED port settings are modified, and the Running Configuration file is updated.
-

Displaying LLDP Port Status

The *LLDP Port Status Table* page displays the LLDP global information for every port.

- To view the LLDP port status, click **Administration > Discovery - LLDP > LLDP Port Status**. The *LLDP Port Status* page opens.
- Click **LLDP Local Information Details** to see the details of the LLDP and LLDP-MED TLVs sent to the neighbor.
- Click **LLDP Neighbor Information Details** to see the details of the LLDP and LLDP-MED TLVs received from the neighbor.

LLDP Port Status Global Information

LLDP Port Status Global Information

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

LLDP Port Status Table

LLDP Port Status Table

- **Interface**—Port identifier.
- **LLDP Status**—LLDP publishing option.
- **LLDP MED Status**—Enabled or disabled.

- **Local PoE**—Local PoE information advertised.
- **Remote PoE**—PoE information advertised by the neighbor.
- **# of neighbors**—Number of neighbors discovered.
- **Neighbor Capability of 1st Device**—Displays the primary functions of the neighbor, for example: Bridge or Router.

Displaying LLDP Local Information

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

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

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

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

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

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

This page provides the following fields:

Global

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

Management Address

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

- **Address Subtype**—Type of management IP address that is listed in the Management Address field, for example, IPv4.

- **Address**—Returned address most appropriate for management use, .
- **Interface Subtype**—Numbering method used for defining the interface number.
- **Interface Number**—Specific interface associated with this management address.

MAC/PHY Details

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

802.3 Details

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

802.3 Link Aggregation

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

802.3 Energy Efficient Ethernet (EEE) (If device supports EEE)

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

- **Remote Rx Echo**—Indicates the local link partner's reflection of the remote link partner's Rx value.

MED Details

- **Capabilities Supported**—MED capabilities supported on the port.
- **Current Capabilities**—MED capabilities enabled on the port.
- **Device Class**—LLDP-MED endpoint device class. The possible device classes are:
 - *Endpoint Class 1*—Indicates a generic endpoint class, offering basic LLDP services.
 - *Endpoint Class 2*—Indicates a media endpoint class, offering media streaming capabilities, as well as all Class 1 features.
 - *Endpoint Class 3*—Indicates a communications device class, offering all Class 1 and Class 2 features plus location, 9 1 1, Layer 2 switch support, and device information management capabilities.
- **PoE Device Type**—Port PoE type, for example, powered.
- **PoE Power Source**—Port power source.
- **PoE Power Priority**—Port power priority.
- **PoE Power Value**—Port power value.
- **Hardware Revision**—Hardware version.
- **Firmware Revision**—Firmware version.
- **Software Revision**—Software version.
- **Serial Number**—Device serial number.
- **Manufacturer Name**—Device manufacturer name.
- **Model Name**—Device model name.
- **Asset ID**—Asset ID.

Location Information

- **Civic**—Street address.
- **Coordinates**—Map coordinates: latitude, longitude, and altitude.

- **ECS ELIN**—Emergency Call Service (ECS) Emergency Location Identification Number (ELIN).

Network Policy Table

- **Application Type**—Network policy application type, for example, Voice.
- **VLAN ID**—VLAN ID for which the network policy is defined.
- **VLAN Type**—VLAN type for which the network policy is defined. The possible field values are:
 - *Tagged*—Indicates the network policy is defined for tagged VLANs.
 - *Untagged*—Indicates the network policy is defined for untagged VLANs.
- **User Priority**—Network policy user priority.
- **DSCP**—Network policy DSCP.

Displaying LLDP Neighbors Information

The *LLDP Neighbors Information* page displays information that was received from neighboring devices.

After timeout (based on the value received from the neighbor Time To Live TLV during which no LLDP PDU was received from a neighbor), the information is deleted.

To view the LLDP neighbors information:

- STEP 1** Click **Administration > Discovery - LLDP > Neighbors Information**. The *LLDP Neighbors Information* page opens.

This page displays the following fields:

- **Local Port**—Number of the local port to which the neighbor is connected.
- **Chassis ID Subtype**—Type of chassis ID (for example, MAC address).
- **Chassis ID**—Identifier of the 802 LAN neighboring device's chassis.
- **Port ID Subtype**—Type of the port identifier that is shown.
- **Port ID**—Identifier of port.
- **System Name**—Published name of the switch.

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

STEP 2 Select a local port, and click **Details**. The *Neighbors Information* page opens.

This page displays the following fields:

Port Details

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

Basic Details

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

Management Address Table

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

MAC/PHY Details

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

802.3 Power via MDI

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

802.3 Details

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

802.3 Link Aggregation

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

802.3 Energy Efficient Ethernet (EEE)

- **Local Tx**—Indicates the time (in micro seconds) that the transmitting link partner waits before it starts transmitting data after leaving Low Power Idle (LPI mode).

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

MED Details

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

802.1 VLAN and Protocol

- **PVID**—Advertised port VLAN ID.

PPVID

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

VLAN IDs

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

Protocol IDs

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

Location Information

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

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

Network Policies

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

Accessing LLDP Statistics

The *LLDP Statistics* page displays LLDP statistical information per port.

To view the LLDP statistics:

-
- STEP 1** Click **Administration > Discovery - LLDP > LLDP Statistics**. The *LLDP Statistics* page opens.

For each port, the fields are displayed:

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

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

LLDP Overloading

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

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

To view LLDP overloading information:

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

This page displays the following fields for each port:

- **Interface**—Port identifier.
- **Total (Bytes)**—Total number of bytes of LLDP information in each packet
- **Left to Send (Bytes)**—Total number of available bytes left for additional LLDP information in each packet.
- **Status**—Whether TLVs are being transmitted or if they are overloaded.

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

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

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

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

Configuring CDP

This section describes how to configure CDP.

It contains the following topics:

- [Setting CDP Properties](#)
- [Editing CDP Interface Settings](#)
- [Displaying CDP Local Information](#)
- [Displaying CDP Neighbors Information](#)
- [Viewing CDP Statistics](#)

Setting CDP Properties

CDP Overview

Similar to LLDP, CDP (Cisco Discovery Protocol) is a link layer protocol for directly connected neighbors to advertise themselves and their capabilities to each other. Unlike LLDP, CDP is a Cisco proprietary protocol.

CDP Configuration Workflow

The following is sample workflow in configuring CDP on the switch. You can also find additional CDP configuration guidelines in the LLDP/CDP section.

- Enter the CDP global parameters using the CDP Properties page
- Configure CDP per interface using the Interface Setting page
- If Auto Smartport is to detect the capabilities of CDP devices, enable CDP in the Smartport Properties page.

See the [Identifying Smartport Type](#) section for a description of how CDP is used to identify devices for the Smartport feature.

The *CDP Properties* page enables entering CDP general parameters.

To enter CDP properties:

STEP 1 Click **Administration > Discovery - CDP > Properties**. The *CDP Properties* page opens.

STEP 2 Enter the parameters.

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

- **Interface**—If *User Defined* was selected for **Source Interface**, select the interface.
- **Syslog Voice VLAN Mismatch**—Check to send a SYSLOG message when a voice VLAN mismatch is detected. This means that the voice VLAN information in the incoming frame does not match what the local device is advertising.
- **Syslog Native VLAN Mismatch**—Check to send a SYSLOG message when a native VLAN mismatch is detected. This means that the native VLAN information in the incoming frame does not match what the local device is advertising.
- **Syslog Duplex Mismatch**—Check to send a SYSLOG message when duplex information is mismatched. This means that the duplex information in the incoming frame does not match what the local device is advertising.

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

Editing CDP Interface Settings

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

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

The LLDP-MED TLVs to be advertised can be selected in the *LLDP MED Interface Settings* page.

To define the LLDP interface settings:

STEP 1 Click **Administration > Discovery - CDP > Interface Settings**. The *Interface Settings* page opens.

This page displays the following CDP information for each interface.

- **CDP Status**—CDP publishing option for the port.
- **Reporting Conflicts with CDP Neighbors**—Displays the status of the reporting options that are enabled/disabled in the **Edit** page.
- **No. of Neighbors**—Number of neighbors detected.

The bottom of the page has four buttons:

- **Copy Settings**—Select to copy a configuration from one port to another.
- **Edit**—Fields explained in Step 2 below.
- **CDP Local Information Details**—Takes you to the *Administration > Discovery - CDP > CDP Local Information* page.
- **CDP Neighbor Information Details**—Takes you to the *Administration > Discovery - CDP > CDP Neighbor Information* page.

STEP 2 Select a port and click **Edit**. The *Edit CDP Interface Settings* page opens.

This page provides the following fields:

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

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

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

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

Displaying CDP Local Information

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

To view the CDP local information:

-
- STEP 1** Click **Administration > Discovery - CDP > CDP Local Information**. The *CDP Local Information* page opens.
- STEP 2** Select a local port, and the following fields are displayed:
- **Interface**—Number of the local port.
 - **CDP State**—Displays whether CDP is enabled or not.
 - **Device ID Type**—Type of the device ID advertised in the device ID TLV.
 - **Device ID**—Device ID advertised in the device ID TLV.
 - **Address(s)**—IP addresses (advertised in the device address TLV).
 - **Port ID**—Identifier of port advertised in the port TLV.
 - **Capabilities**—Capabilities advertised in the port TLV)
 - **Version**—Information about the software release on which the device is running.
 - **Platform**—Identifier of platform advertised in the platform TLV.
 - **Native VLAN**—The native VLAN identifier advertised in the native VLAN TLV.
 - **Duplex**—Whether port is half or full duplex advertised in the full/half duplex TLV.
 - **Appliance ID**—Type of device attached to port advertised in the appliance TLV.
 - **Appliance VLAN ID**—VLAN on the device used by the appliance, for instance if the appliance is an IP phone, this is the voice VLAN.
 - **Extended Trust**—Enabled indicates that the port is trusted, meaning that the host/server from which the packet is received is trusted to mark the packets itself. In this case, packets received on such a port are not re-marked. Disabled indicates that the port is not trusted in which case, the following field is relevant.

- **CoS for Untrusted Ports**—If Extended Trust is disabled on the port, this field displays the Layer 2 CoS value, meaning, an 802.1D/802.1p priority value. This is the COS value with which all packets received on an untrusted port are remarked by the device.
- **Request ID**—Last power request ID received echoes the Request-ID field last received in a Power Requested TLV. It is 0 if no Power Requested TLV was received since the interface last transitioned to Up.
- **Power Management ID**—Value incremented by 1 (or 2, to avoid 0) each time any one of the following events occur:
 - Available-Power or Management Power Level fields change value
 - A Power Requested TLV is received with a Request-ID field which is different from the last-received set (or when the first value is received)
 - The interface transitions to Down
- **Available Power**—Amount of power consumed by port.
- **Management Power Level**—Displays the supplier's request to the powered device for its Power Consumption TLV. The device always displays “No Preference” in this field.

Displaying CDP Neighbors Information

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

After timeout (based on the value received from the neighbor Time To Live TLV during which no CDP PDU was received from a neighbor), the information is deleted.

To view the CDP neighbors information:

- STEP 1** Click **Administration > Discovery - CDP > CDP Neighbors Information**. The *CDP Neighbors Information* page opens.

This page displays the following fields for the link partner (neighbor):

- **Device ID**—Neighbor's device ID.
- **Local Interface**—Number of the local port to which the neighbor is connected.
- **Advertisement Version**—CDP protocol version.

- **Time to Live (sec)**—Time interval (in seconds) after which the information for this neighbor is deleted.
- **Capabilities**—Capabilities advertised by neighbor.
- **Platform**—Information from Platform TLV of neighbor.
- **Neighbor Interface**—Outgoing interface of the neighbor.

STEP 2 Select a device, and click **Details**. The *CDP Neighbors Details* page opens.

This page displays the following fields about the neighbor:

- **Device ID**—Identifier of the neighboring device ID.
- **Local Interface**—Interface number of port through which frame arrived.
- **Advertisement Version**—Version of CDP.
- **Time to Live**—Time interval (in seconds) after which the information for this neighbor is deleted.
- **Capabilities**—Primary functions of the device. The capabilities are indicated by two octets. Bits 0 through 7 indicate Other, Repeater, Bridge, WLAN AP, Router, Telephone, DOCSIS cable device, and station respectively. Bits 8 through 15 are reserved.
- **Platform**—Identifier of the neighbor's platform.
- **Neighbor Interface**—Interface number of the neighbor through which frame arrived.
- **Native VLAN**—Neighbor's native VLAN.
- **Duplex**—Whether neighbors interface is half or full duplex.
- **Addresses**—Neighbor's addresses.
- **Power Drawn**—Amount of power consumed by neighbor on the interface.
- **Version**—Neighbor's software version.

NOTE Clicking on the **Clear Table** button will disconnect all connected devices if from CDP, and if Auto Smartport is enabled will change all port types to default.

Viewing CDP Statistics

The *CDP Statistics* page displays information regarding Cisco Discovery Protocol (CDP) frames that were sent or received from a port. CDP packets are received from devices attached to the switches interfaces, and are used for the Smartport feature. See [Configuring CDP](#) for more information.

CDP statistics for a port are only displayed if CDP is enabled globally and on the port. This is done in the *CDP Properties* page and the *CDP Interface Settings* page.

To view CDP statistics:

- STEP 1** Click **Administration > Discovery - CDP > CDP Statistics**. The *CDP Statistics* page opens.
- STEP 2** Enter the parameter.
 - **Refresh Rate**—Select the time period that passes before the *CDP Statistics* page is refreshed.

The Attribute Counter block displays the counters for various types of packets per interface.

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

The CDP Error Statistics section displays the CDP error counters.

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

To clear the counters, click **Clear Counters**. The CDP Statistics counters are cleared.

Port Management

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

It contains the following topics:

- [Configuring Ports](#)
- [Setting Basic Port Configuration](#)
- [Configuring Link Aggregation](#)
- [Configuring Green Ethernet](#)

Configuring Ports

To configure ports, perform the following actions:

1. Configure port by using the *Port Setting* page.
2. Enable/disable the Link Aggregation Control (LAG) protocol, and configure the potential member ports to the desired LAGs by using the *LAG Management* page. By default, all LAGs are empty.
3. Configure the Ethernet parameters, such as speed and auto-negotiation for the LAGs by using the *LAG Settings* page.
4. Configure the LACP parameters for the ports that are members or candidates of a dynamic LAG by using the *LACP* page.
5. Configure Green Ethernet and 802.3 Energy Efficient Ethernet by using the *Properties* page.
6. Configure Green Ethernet energy mode and 802.3 Energy Efficient Ethernet per port by using the *Port Settings* page.
7. If PoE is supported and enabled for the switch, configure the switch as described in [Managing Power-over-Ethernet Devices](#).

Setting Basic Port Configuration

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

To configure port settings:

-
- STEP 1** Click **Port Management > Port Setting**. The *Port Setting* page opens.
- STEP 2** Select **Jumbo Frames** to support packets of up to 10 Kb in size. If **Jumbo Frames** is not enabled (default), the system supports packet size up to 1,632 bytes. For jumbo frames to take effect, the switch will need to be rebooted after the feature is enabled.
- STEP 3** Click **Apply** to update the global setting.

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

- STEP 4** To update the port settings, select the desired port, and click **Edit**. The *Edit Port Setting* page opens.
- STEP 5** Modify the following parameters:

- **Interface**—Select the port number.
- **Port Description**—Enter the port user-defined name or comment.
- **Port Type**—Displays the port type and speed. The possible options are:
 - *Copper Ports*—Regular, not Combo, support the following values: 10M, 100M, and 1000M (type: Copper).
 - *Combo Ports Copper*—Combo port connected with copper CAT5 cable, supports the following values: 10M, 100M, and 1000M (type: ComboC).
 - *Combo Fiber*—*SFP Fiber Gigabit Interface Converter Port* with the following values: 100M and 1000M (type: ComboF).

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

- **Administrative Status**—Select whether the port should be Up or Down when the switch is rebooted.

- **Operational Status**—Displays whether the port is currently Up or Down.
- **Reactivate Suspended Port**—Select to reactivate a port that has been suspended. There are numerous ways that a port can be suspended, such as through the locked port security option, dot1x single host violation, loopback detection, or STP loopback guard. The reactivate operation brings the port up without regard to why the port was suspended.
- **Auto-Negotiation**—Select to enable auto-negotiation on the port. Auto-negotiation enables a port to advertise its transmission speed, duplex mode, and Flow Control abilities to the port link partner.
- **Operational Auto-Negotiation**—Displays the current auto-negotiation status on the port.
- **Administrative Port Speed**—Configure the speed of the port. The port type determines which the available speeds. You can designate *Administrative Speed* only when port auto-negotiation is disabled.

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

- **Operational Port Speed**—Displays the current port speed that is the result of negotiation.
- **Administrative Duplex Mode**—Select the port duplex mode. This field is configurable only when auto-negotiation is disabled, and the port speed is set to 10M or 100M. At port speed of 1G, the mode is always full duplex. The possible options are:
 - *Full*—The interface supports transmission between the switch and the client in both directions simultaneously.
 - *Half*—The interface supports transmission between the switch and the client in only one direction at a time.
- **Operational Duplex Mode**—Displays the port's current duplex mode.
- **Auto Advertisement**—Select the capabilities advertised by auto-negotiation when it is enabled. The options are:
 - *Max Capability*—All port speeds and duplex mode settings can be accepted.
 - *10 Half*—10 Mbps speed and Half Duplex mode.
 - *10 Full*—10 Mbps speed and Full Duplex mode.

- *100 Half*—100 Mbps speed and Half Duplex mode.
- *100 Full*—100 Mbps speed and Full Duplex mode.
- *1000 Full*—1000 Mbps speed and Full Duplex mode.
- **Operational Advertisement**—Displays the capabilities currently published to the port's neighbor. The possible options are those specified in the *Administrative Advertisement* field.
- **Neighbor Advertisement**—Displays the capabilities advertised by the neighboring device (link partner).
- **Back Pressure**—Select the Back Pressure mode on the port (used with Half Duplex mode) to slow down the packet reception speed when the switch is congested. It disables the remote port, preventing it from sending packets by jamming the signal.
- **Flow Control**—Enable or disable 802.3x Flow Control, or enable the auto-negotiation of Flow Control on the port (only when in Full Duplex mode).
- **MDI/MDIX**—the *Media Dependent Interface (MDI)/Media Dependent Interface with Crossover (MDIX)* status on the port.

The options are:

- *MDIX*—Select to swap the port's transmit and receives pairs.
- *MDI*—Select to connect this switch to a station by using a straight through cable.
- *Auto*—Select to configure this switch to automatically detect the correct pinouts for the connection to another device.
- **Operational MDI/MDIX**—Displays the current MDI/MDIX setting.
- **Member in LAG**—Displays the LAG, if the port is a member of a LAG; otherwise this field is left blank.

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

Configuring Link Aggregation

This section describes how to configure LAGs. It contains the following topics:

- [Link Aggregation Overview](#)
- [Static and Dynamic LAG Workflow](#)
- [Defining LAG Management](#)
- [Configuring LAG Settings](#)
- [Configuring LACP](#)

Link Aggregation Overview

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

Two types of LAGs are supported:

- *Static*—A LAG is static if the LACP is disabled on it. The group of ports assigned to a static LAG are always active members. After a LAG is manually created, the LACP option cannot be added or removed, until the LAG is edited and a member is removed (which can be added prior applying), then the LACP button will become available for editing.
- *Dynamic*—A LAG is dynamic if LACP is enabled on it. The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports. The non-active candidate ports are *standby* ports ready to replace any failing active member ports.

Load Balancing

Load Balancing

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

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

The switch supports two modes of load balancing:

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

LAG Management

LAG Management

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

The switch supports four LAGs.

Every LAG has the following characteristics:

- All ports in a LAG must be of the same media type.
- To add a port to the LAG, it cannot belong to any VLAN except the default VLAN.
- Ports in a LAG must not be assigned to another LAG.
- No more than eight ports are assigned to a static LAG and no more than 16 ports can be candidates for a dynamic LAG.
- All the *ports* in a LAG must have auto-negotiation disabled, although the *LAG* can have auto-negotiation enabled.
- When a port is added to a LAG, the configuration of the LAG is applied to the port. When the port is removed from the LAG, its original configuration is reapplied.
- Protocols, such as Spanning Tree, consider all the ports in the LAG to be one port.

Static and Dynamic LAG Workflow

NOTE After a LAG has been manually created, LACP cannot be added or removed until the LAG is edited and a member is removed. Only then will the LACP button become available for editing.

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

1. Disable LACP on the LAG to make it static. Assign up to eight member ports to the static LAG by selecting and moving the ports from the **Port List** to the **LAG Members** list. Select the load balancing algorithm for the LAG. Perform these actions in the *LAG Management* page.
2. Configure various aspects of the LAG, such as speed and flow control by using the *LAG Settings* page.

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

1. Enabling LACP on the LAG. Assign up to 16 candidates ports to the dynamic LAG by selecting and moving the ports from the **Port List** to the **LAG Members** List by using the *LAG Management* page.
2. Configure various aspects of the LAG, such as speed and flow control by using the *LAG Settings* page.
3. Set the LACP priority and timeout of the ports in the LAG by using the *LACP* page.

Defining LAG Management

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

To select the load balancing algorithm of the LAG:

-
- STEP 1** Click **Port Management > Link Aggregation > LAG Management**. The *LAG Management* page opens.
- STEP 2** Select one of the following **Load Balance Algorithms**:
- *MAC Address*—Perform load balancing by source and destination MAC addresses on all packets.
 - *IP/MAC Address*—Perform load balancing by the source and destination IP addresses on IP packets, and by the source and destination MAC addresses on non-IP packets
- STEP 3** Click **Apply**. The Load Balance Algorithm is defined, and the Running Configuration file is updated.
-

To define the member or candidate ports in a LAG.

-
- STEP 1** Select the LAG to be configured, and click **Edit**. The *Edit LAG Membership* page opens.
- STEP 2** Enter the values for the following fields:
- **LAG**—Select the LAG number.
 - **LAG Name**—Enter the LAG name or a comment.
 - **LACP**—Select to enable LACP on the selected LAG. This makes it a dynamic LAG. This field can only be enabled after moving a port to the LAG in the next field.
 - **Port List**—Move those ports that are to be assigned to the LAG from the **Port List** to the **LAG Members** list. Up to eight ports per static LAG can be assigned, and 16 ports can be assigned to a dynamic LAG.
- STEP 3** Click **Apply**. The LAG membership is defined, and the Running Configuration file is updated.
-

Configuring LAG Settings

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

To configure the LAG settings or reactivate a suspended LAG:

-
- STEP 1** Click **Port Management > Link Aggregation > LAG Settings**. The *LAG Settings* page opens.
- STEP 2** Select a LAG, and click **Edit**. The *Edit LAG Settings* page opens.
- STEP 3** Enter the values for the following fields:
- **LAG**—Select the LAG ID number.
 - **Description**—Enter the LAG name or a comment.
 - **LAG Type**—Displays the port type that comprises the LAG.
 - **Administrative Status**—Set the selected LAG to be Up or Down.
 - **Operational Status**—Displays whether the LAG is currently operating.

- **Reactivate Suspended LAG**—Select to reactivate a port if the LAG has been disabled through the locked port security option .
- **Administrative Auto-Negotiation**—Enables or disable auto-negotiation on the LAG. Auto-negotiation is a protocol between two link partners that enables a LAG to advertise its transmission speed and flow control to its partner (the Flow Control default is *disabled*). It is recommended to keep auto-negotiation enabled on both sides of an aggregate link, or disabled on both sides, while ensuring that link speeds are identical.
- **Operational Auto-Negotiation**—Displays the auto-negotiation setting.
- **Administrative Speed**—Select the LAG speed.
- **Operational LAG Speed**—Displays the current speed at which the LAG is operating.
- **Administrative Advertisement**—Select the capabilities to be advertised by the LAG. The options are:
 - *Max Capability*—All LAG speeds and both duplex modes are available.
 - *10 Full*—The LAG advertises a 10 Mbps speed and the mode is full duplex.
 - *100 Full*—The LAG advertises a 100 Mbps speed and the mode is full duplex.
 - *1000 Full*—The LAG advertises a 1000 Mbps speed and the mode is full duplex.
- **Operational Advertisement**—Displays the Administrative Advertisement status. The LAG advertises its capabilities to its neighbor LAG to start the negotiation process. The possible values are those specified in the *Administrative Advertisement* field.
- **Neighbor Advertisement**—Displays the capabilities that are advertised by the neighbor LAG (the LAG to which the selected interface is connected) that advertises its capabilities to the LAG to start the negotiation process. The values are the same as in the Administrative Advertisement field.
- **Administrative Flow Control**—Enable or disable Flow Control or enable the auto-negotiation of Flow Control on the LAG.
- **Operational Flow Control**—Displays the current Flow Control setting.

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

Configuring LACP

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

LACP Priority and Rules

LACP Priority and Rules

LACP system priority and LACP port priority are both used to determine which of the candidate ports become active member ports in a dynamic LAG configured with more than eight candidate ports.

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

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

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

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

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

Setting Port LACP Parameter Settings

The *LACP* page displays and enables configuration of the LACP System Priority, LACP timeout, and LACP port priority. LACP timeout is a per port parameter, and is the time interval between the sending and receiving of consecutive LACP PDUs. With all factors equal, when the LAG is configured with more candidate ports than the maximum number of active ports allowed, the switch selects ports as active from the dynamic LAG that has the highest priority

NOTE The LACP setting is irrelevant on ports that are not members of a dynamic LAG.

To define the LACP settings:

-
- STEP 1** Click **Port Management > Link Aggregation > LACP**. The *LACP* page opens.
- STEP 2** Select a port, and click **Edit**. The *Edit LACP* page opens.
- STEP 3** Enter the values for the following fields:
- **Port**—Select the port number to which timeout and priority values are assigned.
 - **LACP Port Priority**—Enter the LACP priority value for the port.
 - **LACP Timeout**—Select the periodic transmissions of LACP PDUs, which occur at either a long or short transmission speed, depending upon the expressed LACP timeout preference.
- STEP 4** Click **Apply**. The Running Configuration file is updated.
-

Configuring Green Ethernet

This section describes the Green Ethernet feature that is designed to save power on the switch.

It contains the following sections:

- [Green Ethernet Overview](#)
- [Setting Global Green Ethernet Properties](#)
- [Setting Green Ethernet Properties for Ports](#)

Green Ethernet Overview

Green Ethernet is a common name for a set of features that is designed to be environmentally friendly, and to reduce the power consumption of a device. Green Ethernet is different from EEE in that green ethernet energy-detect is enabled on all devices where only the Gigabyte ports are enable with EEE.

The Green Ethernet feature can reduce overall power usage in the following ways:

- **Energy-Detect Mode**—On an inactive link, the port moves into inactive mode, saving power while keeping the Administrative status of the port Up. Recovery from this mode to full operational mode is fast, transparent, and no frames are lost. This mode is supported on both GE and FE ports.
- **Short-Reach Mode**—This feature provides for power savings on a short length of cable. After cable length is analyzed, the power usage is adjusted for various cable lengths. If the cable is shorter than 50 meters, the switch uses less power to send frames over the cable, thus saving energy. This mode is only supported on RJ45 GE ports; it does not apply to Combo ports.

This mode is globally disabled by default. It cannot be enabled if EEE mode is enabled (see below).

In addition to the above Green Ethernet features, the **802.3az Energy Efficient Ethernet (EEE)** is found on devices supporting GE ports. EEE reduces power consumption when there is no traffic on the port. See the [802.3az Energy Efficient Ethernet Feature](#) section for more information (available on GE models only).

EEE is enabled globally by default. On a given port, if EEE is enabled, short reach mode will be disabled. If Short Reach Mode is enabled, EEE will be grayed out regardless of the Short Reach Mode global status.

These modes are configured per port, without taking into account the LAG membership of the ports.

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

802.3az Energy Efficient Ethernet Feature

This section describes the 802.3az Energy Efficient Ethernet (EEE) feature.

It contains the following topics:

- [802.3az EEE Overview](#)
- [Advertise Capabilities Negotiation](#)
- [Link Level Discovery for 802.3az EEE](#)
- [Availability of 802.3az EEE](#)
- [Default Configuration](#)
- [Interactions Between Features](#)
- [802.3az EEE Configuration Workflow](#)

802.3az EEE Overview

802.3az EEE is designed to save power when there is no traffic on the link. In Green Ethernet, power is reduced when the port is down. With 802.3az EEE, power is reduced when the port is up, but there is no traffic on it.

802.3az EEE is only supported on devices with GE ports.

When using 802.3az EEE, systems on both sides of the link can disable portions of their functionality and save power during periods of no traffic.

802.3az EEE supports IEEE 802.3 MAC operation at 100 Mbps and 1000 Mbps:

LLDP is used to select the optimal set of parameters for both devices. If LLDP is not supported by the link partner, or is disabled, 802.3az EEE will still be operational, but it might not be in the optimal operational mode.

The 802.3az EEE feature is implemented using a port mode called Low Power Idle (LPI) mode. When there is no traffic and this feature is enabled on the port, the port is placed in the LPI mode, which reduces power consumption dramatically.

Both sides of a connection (switch port and connecting device) must support 802.3az EEE for it to work. When traffic is absent, both sides send signals indicating that power is about to be reduced. When signals from both sides are received, the Keep Alive signal indicates that the ports are in LPI status (and not in Down status), and power is reduced.

For ports to stay in LPI mode, the Keep Alive signal must be received continuously from both sides.

Advertise Capabilities Negotiation

802.3az EEE support is advertised during the Auto-Negotiation stage. Auto-Negotiation provides a linked device with the capability to detect the abilities (modes of operation) supported by the device at the other end of the link, determine common abilities, and configure itself for joint operation. Auto-Negotiation is performed at the time of link-up, on command from management, or upon detection of a link error. During the link establishment process, both link partners exchange their 802.3az EEE capabilities. Auto-Negotiation functions automatically without user interaction when it is enabled on the device.

NOTE If Auto-Negotiation is not enabled on a port, the EEE is disabled. The only exception is if the link speed is 1GB, then EEE will still be enabled even though Auto-Negotiation is disabled.

Link Level Discovery for 802.3az EEE

In addition to the capabilities described above, 802.3az EEE capabilities and settings are also advertised using frames based on the organizationally-specific TLVs defined in Annex G of IEEE Std 802.1AB protocol (LLDP). LLDP is used to further optimize 802.3az EEE operation after auto-negotiation is completed. The 802.3az EEE TLV is used to fine tune system wake-up and refresh durations.

Availability of 802.3az EEE

Please check the release notes for a complete listing of products that support EEE.

Default Configuration

By default, 802.3az EEE and EEE LLDP are enabled globally and per port.

Interactions Between Features

The following describe 802.3az EEE interactions with other features:

- If auto-negotiation is not enabled on the port, the 802.3az EEE operational status is disabled. The exception to this rule is that if the link speed is

1gigabyte, EEE will still be enabled even though Auto-Negotiation is disabled.

- If 802.3az EEE is enabled and the port is going Up, it commences to work immediately in accordance with the maximum wake time value of the port.
- On the GUI, the EEE field for the port is not available when the Short Reach Mode option on the port is checked.
- If the port speed on the GE port is changed to 10Mbit, 802.3az EEE is disabled. This is supported in GE models only.

802.3az EEE Configuration Workflow

This section describes how to configure the 802.3az EEE feature and view its counters.

-
- STEP 1** Ensure that auto-negotiation is enabled on the port by opening the Port Management > *Port Settings* page.
 - a. Select a port and open the *Edit Port Settings* page.
 - b. **Select the Operational Auto Negotiation** field to ensure that it is Enabled.
 - STEP 2** Ensure that **803.2 Energy Efficient Ethernet (EEE)** is globally enabled in the Port Management > Green Ethernet > *Properties* page (it is enabled by default). This page also displays how much energy has been saved.
 - STEP 3** Ensure that 802.3az EEE is enabled on a port by opening the Green Ethernet > *Port Settings* page.
 - a. Select a port, open the *Edit Port Settings* page.
 - b. Check the **802.3 Efficient Energy Ethernet (EEE)** mode on the port (it is enabled by default).
 - c. Select whether to enable or disable advertisement of 802.3az EEE capabilities through LLDP in **802.3 Efficient Energy Ethernet (EEE) LLDP** (it is enabled by default).
 - STEP 4** To see 802.3az EEE-related information on the local device, open the *Administration > Discovery LLDP > LLDP Local Information* page, and view the information in the 802.3az Energy Efficient Ethernet (EEE) block.
 - STEP 5** To display 802.3az EEE information on the remote device, open the *Administration > Discovery LLDP > LLDP Neighbor Information* pages, and view the information in the 802.3 Energy Efficient Ethernet (EEE) block.

Setting Global Green Ethernet Properties

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

To enable Green Ethernet and EEE and view power savings:

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

STEP 2 Enter the values for the following fields:

- **Energy Detect Mode**—Globally enable or disable Energy Detect mode. If this mode is changed, a message is displayed. (Energy Detect Mode does not need to be enabled for EEE to function).

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

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

- **Short Reach**—Globally enable or disable Short Reach mode if there are GE ports on the switch. If this mode is changed, a message is displayed. The field still shows on switches that do not have GE ports, but is invalid.
- **802.3 Energy Efficient Ethernet (EEE)**— Globally enable or disable EEE mode (only available if there are GE ports on the switch). If this mode is changed, a message is displayed.
- **Power Savings**—Displays the amount of power saved by running in Green Ethernet mode.
- **Cumulative Energy Saved**—Displays the amount of energy saved from the last switch reboot. This value is updated each time there is an event that affects power saving. (This value does not take into consideration the amount of energy saved with the use of EEE).

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

Setting Green Ethernet Properties for Ports

The *Port Settings* page displays the current Green Ethernet and EEE modes per port, and enables configuring Green Ethernet on a port using the *Edit Port Setting* page. For the Green Ethernet modes to operate on a port, the corresponding modes must be activated globally in the *Properties* page.

Note that EEE settings are only displayed for devices that have GE ports. EEE works only when ports are set to Auto negotiation. The exception is that EEE is still functional even when Auto Negotiation is disabled, but the port is at 1GB or higher.

To define per port Green Ethernet settings:

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

The *Port Settings* page displays the following:

- **Port**—The port number.
 - **Energy Detect**—State of the port regarding Energy Detect mode:
 - *Administrative*—Displays whether Energy Detect mode was enabled.
 - *Operational*—Displays whether Energy Detect mode is currently operating.
 - *Reason*—If Energy Detect mode is not operational, displays the reason.
 - **Short Reach**—State of the port regarding Short Reach mode:
 - *Administrative*—Displays whether Short Reach mode was enabled.
 - *Operational*—Displays whether Short Reach mode is currently operating.
 - *Reason*—If Short-Reach mode is not operational, displays the reason.
 - *Cable Length*—Displays VCT-returned cable length in meters.
- NOTE** Short-reach mode is only supported on RJ45 GE ports; it does not apply to Combo ports.
- **802.3 Energy Efficient Ethernet (EEE)**—State of the port regarding the EEE feature:
 - *Administrative*—Displays whether EEE was enabled.

- *Operational*—Displays whether EEE is currently operating on the local port. This is a function of whether it has been enabled (Administrative Status), whether it has been enabled on the local port and whether it is operational on the local port.
- *LLDP Administrative*—Displays whether advertising EEE counters through LLDP was enabled.
- *LLDP Operational*—Displays whether advertising EEE counters through LLDP is currently operating.
- *EEE Support on Remote*—Displays whether EEE is supported on the link partner. EEE must be supported on both the local and remote link partners.

NOTE The window displays the Short Reach, Energy Detect and EEE settings for each port; however, they are not enabled on any port unless they are also enabled globally by using the *Properties* page. To enable Short Reach and EEE globally, see the *Setting Global Green Ethernet Properties* section.

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

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

STEP 4 Select to enable or disable Short Reach mode on the port if there are GE ports on the device.

STEP 5 Select to enable or disable 802.3 Energy Efficient Ethernet (EEE) mode on the port if there are GE ports on the device.

STEP 6 Select to enable or disable 802.3 Energy Efficient Ethernet (EEE) LLDP mode on the port (advertisement of EEE capabilities through LLDP) if there are GE ports on the device.

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

Smartports

This document describes the Smartports feature.

It contains the following topics:

- **Overview**
- **What is a Smartport**
- **Smartport Types**
- **Smartport Macros**
- **How the Smartport Feature Works**
- **Macro Failure and the Reset Operation**
- **Auto Smartport**
- **Default Configuration**
- **Relationships with Other Features and Backwards Compatibility**
- **Common Smartport Tasks**
- **Web GUI**
- **Built-in Smartport Macros**

Overview

The Smartport feature provides a convenient way to save and share common configurations. By applying the same Smartport macro to multiple interfaces, the interfaces share a common set of configurations.

A Smartport macro can be applied to an interface by the Smartport type associated with the macro.

There are two ways to apply a Smartport macro by Smartport type to an interface:

- **Static Smartport**—The user manually assigns a Smartport type to an interface. The result is the corresponding Smartport macro is applied to the interface.
- **Auto Smartport**—Auto Smartport waits for a device to be attached to the interface before applying a configuration. When a device is detected from an interface, the Smartport macro (if assigned) that corresponds to the Smartport type of the attaching device is automatically applied.

The Smartport feature consists of various components and works in conjunction with other features on the switch. These components and features are described in the following sections:

- Smartport, Smartport types and Smartport macros, described in this section.
- Voice VLAN and Smartport, described in the [Voice VLAN](#) section.
- LLDP/CDP for Smartport, described in the [Configuring LLDP](#) and [Configuring CDP](#) sections, respectively.

Additionally, typical work flows are described in the [Common Smartport Tasks](#) section.

What is a Smartport

A Smartport is an interface to which a built-in macro may be applied. These macros are designed to provide a means of quickly configuring the switch to support the communication requirements and utilize the features of various types of network devices. The network access and QoS requirements vary if the interface is connected to an IP phone, a printer, or a router and/or Access Point (AP).

Smartport Types

Smartport types refers to the types of devices attached, or to be attached to Smartports. The switch supports the following Smartport types:

- Printer

- Desktop
- Guest
- Server
- Host
- IP Camera
- IP phone
- IP Phone+Desktop
- Switch
- Router
- Wireless Access Point

Smartport types are named so that they describe the type of device connected to an interface. Each Smartport type is associated with two Smartport macros. One macro, called "the macro," serves to apply the desired configuration. The other, called "the anti-macro," serves to undo all configuration performed by "the macro" when that interface happens to become a different Smartport type.

A Smartport macro can be applied by its Smartport type statically from the GUI, and dynamically by Auto Smartport. Auto Smartport derives the Smartport types of the attached devices based on CDP capabilities, LLDP system capabilities, and/or LLDP-MED capabilities.

Table 1 describes the relationship of Smartport types and Auto Smartport

Table 1

Smartport Type	Supported by Auto Smartport	Supported by Auto Smartport by default
Unknown	No	No
Default	No	No
Printer	No	No
Desktop	No	No
Guest	No	No

Table 1

Smartport Type	Supported by Auto Smartport	Supported by Auto Smartport by default
Server	No	No
Host	Yes	No
IP camera	No	No
IP phone	Yes	Yes
IP phone desktop	Yes	Yes
Switch	Yes	Yes
Router	Yes	No
Wireless Access Point	Yes	Yes

Special Smartport Types

There are two special smartport types; "default" and "unknown." These two types are not associated with macros, but they exist to signify the state of the interface regarding smartport.

The following are special Smartport types:

- **Default**

An interface that does not (yet) have a Smartport type assigned to it has the Default Smartport status.

If Auto Smartport assigns a Smartport type to an interface and the interface is not configured to be Auto Smartport Persistent, then its Smartport type will be re-initialized to Default in the following cases:

- A link down/up operation is performed on the interface.
- The switch is restarted.
- All devices attached to the interface have aged out, which is defined as the absence of CDP and/or LLDP advertisement from the device for a specified time period.

- **Unknown**

If a Smartport macro is applied to an interface and an error occurs, the interface is assigned the Unknown status. In this case, the Smartport and Auto Smartport features do not function on the interface until the user corrects the error and applies the Reset action (performed in the *Edit Interface Settings* page) that resets the Smartport status.

See the workflow area in [Common Smartport Tasks](#) section for troubleshooting tips.

NOTE Throughout this section, the term “aged out” is used to describe the LLDP and CDP messages via their TTL. If Auto Smartport is enabled, and persistent status is disabled, and no more CDP or LLDP messages are received on the interface before both TTLs of the most recent CDP and LLDP packets decrease to 0, then the anti-macro will run and the Smartport type will return to default.

Smartport Macros

A Smartport macro is a script of commands that configure an interface appropriately for a particular network device.

Smartport macros should not be confused with global macros. Global macros configure the switch globally, however, the scope of a Smartport macro is limited to the interface on which it is applied.

The macro source may be found by clicking the *view macro source* button on the Smartport Type Settings page.

A macro and the corresponding anti-macro are paired together in association with each Smartport type. The macro applies the configuration and the anti-macro removes it.

Two Smartport macros are paired by their names as follows:

- macro_name (for example: printer)
- no_macro_name (for example: no_printer, the anti Smartport macro of Smartport macro printer)

See the **Built-in Smartport Macros** section for a listing of the built-in Smartport macros for each device type.

Applying a Smartport Type to an Interface

When Smartport types are applied to interfaces, the smartport types and configuration in the associated Smartport macros are saved in the Running Configuration File. If the administrator saves the Running Configuration File into the Startup Configuration File, the switch will apply the Smartport types and the Smartport macros to the interfaces after reboot as follows:

- If the Startup Configuration File does not specify a Smartport type for an interface, its Smartport type is set to Default.
- If the Startup Configuration File specifies a static Smartport type, the Smartport type of the interface is set to this static type.
- If the Startup Configuration File specifies a Smartport type that was dynamically assigned by Auto Smartport:
 - If the Auto Smartport Global Operational state, the interface Auto Smartport state, and the Persistent Status are all Enable, the Smartport type is set to this dynamic type.
 - Else the corresponding anti-macro is applied and the interfaces status is set to Default.

Macro Failure and the Reset Operation

A Smartport macro may fail if there is a conflict between the existing configuration of the interface and a Smartport macro.

When a Smartport macro fails, a SYSLOG message containing the following parameters is sent:

- Port number
- Smartport type
- The line number of the failed CLI command in the macro

When a Smartport macro fails on an interface, the status of the interface is set to *Unknown*. The reason for the failure can be displayed in the *Interface Settings* page, **Show Diagnostics** popup.

After the source of the problem is determined and the existing configuration or Smartport macro is corrected, you must perform a reset operation to reset the interface before it can be reapplied with a Smartport type (in the *Interface Settings, Edit* page). See the workflow area in **Common Smartport Tasks** section for troubleshooting tips.

How the Smartport Feature Works

You can apply a Smartport macro to an interface by the Smartport type associated with the macro. Because support is provided for Smartport types which correspond to devices which do not allow themselves to be discovered via CDP and/or LLDP, these Smartport types must be statically assigned to the desired interfaces. This can be done by navigating to the Smartport Interface Settings page, selecting the radio button of the desired interface, and clicking edit. Then select the Smartport type you want to assign and adjust the parameters as necessary before clicking apply.

There are two ways to apply Smartport macro by Smartport type to an interface:

- **Static Smartport**

The user manually assigns a Smartport type to an interface. The corresponding Smartport macro is applied to the interface. You can manually assign a Smartport type to an interface from the *Smartport Interface Settings Page*.

- **Auto Smartport**

When a device is detected from an interface, the Smartport macro, if any, that corresponds to the Smartport type of the attaching device is automatically applied. Auto Smartport is enabled by default globally, and at the interface level.

In both cases, the associated anti-macro is run when the Smartport type is removed from the interface, and the anti-macro runs in exactly the same manner, removing all of the configuration.

Auto Smartport

In order for Auto Smartport to automatically assign Smartport types to interfaces, the Auto Smartport feature must be enabled globally and on the interfaces which Auto Smartport should be allowed to configure. By default, Auto Smartport is enabled and allowed to configure all interfaces. The Smartport type assigned to each interface is determined by the CDP and LLDP packets received on the each interface respectively.

- If multiple devices are attached to an interface, a configuration profile that is appropriate for all of the devices is applied to the interface if possible.
- If a device is aged out (no longer receiving advertisements from other devices), the interface configuration is changed according to its Persistent Status. If the Persistent Status is enabled, the interface configuration is retained. If not, the Smartport Type reverts to Default.

Enabling Auto Smartport

Enabling Auto Smartport

Auto Smartport can be enabled globally in the *Properties* page in the following ways:

- **Enabled**—This manually enables Auto Smartport and places it into operation immediately.
- **Enable by Auto Voice VLAN**—This enables Auto Smartport to operate if, and only if, Auto Voice VLAN is enabled and in operation. Enable by Auto Voice VLAN is the default.

NOTE In addition to enabling Auto Smartport globally, you need to enable Auto Smartport at the desired interface as well. By default, Auto Smartport is enabled at all the interfaces.

See the **Voice VLAN** section for more information on enabling Auto Voice VLAN

Identifying Smartport Type

If Auto Smartport is globally enabled (in the *Properties* page), and at an interface (in the *Interface Settings* page), the switch applies a SmartPort macro to the interface based on the Smartport type of the attaching device. Auto SmartPort derives the SmartPort types of attaching devices based on the CDP and/or LLDP the devices advertise.

If, for example, an IP phone is attached to a port, it transmits CDP or LLDP packets that advertise its capabilities. After reception of these CDP and/or LLDP packets, the switch derives the appropriate SmartPort type for phone and applies the corresponding SmartPort macro to the interface where the IP phone attaches.

Unless Persistent Auto SmartPort is enabled on an interface, the SmartPort type and resulting configuration applied by Auto SmartPort will be removed if the attaching device(s) ages out, links down, reboots, or conflicting capabilities are received. Aging out times are determined by the absence of CDP and/or LLDP advertisements from the device for a specified time period.

Using CDP/LLDP Information to Identify Smartport Types

The switch detects the type of device attached to the port, based on the CDP/LLDP capabilities.

This mapping is shown in [Table 2](#) and [Table 3](#).

Table 2 CDP Capabilities Mapping to Smartport Type

Capability Name	CDP Bit	Smartport Type
Router	0x01	Router
TB Bridge	0x02	Wireless Access Point
SR Bridge	0x04	Ignore
Switch	0x08	Switch
Host	0x10	Host
IGMP conditional filtering	0x20	Ignore
Repeater	0x40	Ignore
VoIP Phone	0x80	ip_phone
Remotely-Managed Device	0x100	Ignore
CAST Phone Port	0x200	Ignore

Table 2 CDP Capabilities Mapping to Smartport Type (Continued)

Capability Name	CDP Bit	Smartport Type
Two-Port MAC Relay	0x400	Ignore

Table 3 LLDP Capabilities Mapping to Smartport Type

Capability Name	LLDP Bit	Smartport Type
Other	1	Ignore
Repeater IETF RFC 2108	2	Ignore
MAC Bridge IEEE Std 802.1D	3	Switch
WLAN Access Point IEEE Std 802.11 MIB	4	Wireless Access Point
Router IETF RFC 1812	5	Router
Telephone IETF RFC 4293	6	ip_phone
DOCSIS cable device IETF RFC 4639 and IETF RFC 4546	7	Ignore
Station Only IETF RFC 4293	8	Host
C-VLAN Component of a VLAN Bridge IEEE Std 802.1Q	9	Switch
S-VLAN Component of a VLAN Bridge IEEE Std 802.1Q	10	Switch
Two-port MAC Relay (TPMR) IEEE Std 802.1Q	11	Ignore
Reserved	12-16	Ignore

NOTE If only the IP Phone and Host bits are set, then the SmartPort type is ip_phone_desktop.

Multiple Devices Attached to the Port

The switch derives the SmartPort type of a connected device via the capabilities the device advertises in its CDP and/or LLDP packets.

If multiple devices are connected to the switch through one interface, Auto Smartport will consider each capability advertisement it receives through that interface in order to assign the correct Smartport type. The assignment is based on the following algorithm:

- If all devices on an interface advertise the same capability (there is no conflict) the matching Smartport type is applied to the interface.
- If one of the devices is a switch, the *Switch* Smartport type is used.
- If one of the devices is an AP, the *Wireless Access Point* Smartport type is used.
- If one of the devices is an IP phone and another device is a host, the *ip_phone_desktop* Smartport type is used.
- If one of the devices is an IP phone desktop and the other is an IP phone or host, the *ip_phone_desktop* Smartport type is used.
- In all other cases the default Smartport type is used.

For more information about LLDP/CDP refer to the [Configuring LLDP](#) and [Configuring CDP](#) sections, respectively.

Persistent Auto Smartport Interface

If the Persistent Status of an interface is enabled, its Smartport type and the configuration that is already applied dynamically by Auto Smartport will remain on the interface even after the attaching device ages out, the interface goes down, and the switch is rebooted (assuming the configuration is being saved). The SmartPort type and the configuration of the interface are not changed unless Auto Smartport detects an attaching device with a different Smartport. If the Persistent Status of an interface is disabled, the interface reverts to the default Smartport type when the attaching device to it ages out, the interface goes down, or the switch is rebooted. Enabling Persistent Status on an interface eliminates the device detection delay that otherwise will occur.

NOTE The persistence of the Smartport types applied to the interfaces are effective between reboots only if the running configuration with the Smartport type applied at the interfaces are saved to the startup configuration file.

Error Handling

When a smart port macro fails to apply to an interface, you can examine the point of the failure in the *Interface Settings* Page and reset the port and reapply the macro after the error is corrected from the *Interface Settings Edit* Page.

Default Configuration

Smartport is always available. By default, Auto Smartport is enabled by Auto Voice VLAN, relies on both CDP and LLDP to detect attaching device's Smartport type, and detects Smartport type IP phone, IP phone + Desktop, Switch, and Wireless Access Point.

See the [Voice VLAN](#) section for a description of the voice factory defaults.

Relationships with Other Features and Backwards Compatibility

Auto Smartport is enabled by default and may be disabled. Telephony OUI cannot function concurrently with Auto Smartport and Auto Voice VLAN. Auto Smartport must be disabled before enabling Telephony OUI.

A switch can be upgraded to support Smartport and Auto Smartport if it does not already support them.

NOTE When upgrading from a firmware level that does not support Auto Smartport to a firmware level that supports Auto Smartport, the Auto Voice VLAN is disabled after the upgrade. If Telephony OUI was enabled before the upgrade, then Auto Smartport is disabled after the upgrade, and Telephony OUI remains enabled.

Common Smartport Tasks

This section describes some common tasks to setup Smartport and Auto Smartport.

Workflow1: *To globally enable Auto Smartport on the switch, and to configure a port with Auto Smartport, perform the following steps:*

-
- STEP 1** To enable the Auto Smartport feature on the switch, open the *Smartport > Properties* page. Set **Administrative Auto Smartport** to **Enable** or **Enable by Voice VLAN**.
 - STEP 2** Select whether the switch is to process CDP and/or LLDP advertisements from connected devices.
 - STEP 3** Select which type of devices will be detected in the **Auto Smartport Device Detection** field.
 - STEP 4** Click **Apply**
 - STEP 5** To enable the Auto Smartport feature on one or more interfaces, open the *Smartport > Interface Settings* page.
 - STEP 6** Select the interface, and click *Edit*.
 - STEP 7** Select Auto Smartport in the **Smartport Application** field.
 - STEP 8** Check or uncheck **Persistent Status** if desired.
 - STEP 9** Click **Apply**.

Workflow2: *To configure an interface as a static Smartport, perform the following steps:*

-
- STEP 1** To enable the Smartport feature on the interface, open the *Smartport > Interface Settings* page.
 - STEP 2** Select the interface, and click *Edit*.
 - STEP 3** Select the Smartport type that is to be assigned to the interface in the **Smartport Application** field.
 - STEP 4** Set the macro parameters as required.
 - STEP 5** Click **Apply**.

Workflow3: *To adjust Smartport macro parameter defaults, perform the following steps:*

Through this procedure you can accomplish the following:

- View the macro source.
 - Change parameter defaults.
 - Restore the parameter defaults to the factory settings.
 -
1. Open the *Smartport > Smartport Type Settings* page.
 2. Select the Smartport Type.
 3. Click **View Macro Source** to view the current Smartport macro that is associated with the selected Smartport Type.
 4. Click **Edit** to open a new window in which you can modify the default values of the parameters in the macros bound to that Smartport type. These parameter default values will be used when Auto Smartport applies the selected Smartport type (if applicable) to an interface.
 5. In the *Edit* page, modify the fields.
 6. Click **Apply** to rerun the macro if the parameters were changed, or **Restore Defaults** to restore default parameter values to built-in macros if required.

Workflow4: *To rerun a Smartport macro after it has failed, perform the following steps:*

-
- STEP 1** In the *Interface Settings* page, select an interface with Smartport Type Unknown.
 - STEP 2** Click **Show Diagnostics** to see the problem.
 - STEP 3** Troubleshoot, then correct the problem. See the troubleshooting tip below.
 - STEP 4** Click **Edit**. A new window will open in which you can click **Reset** to reset the interface.
 - STEP 5** Reapply the Smartport Macro to the interface.

A second method of resetting single or multiple unknown interfaces is:

-
- STEP 1** In the *Interface Settings* page, select the *Port Type* equals to checkbox.
 - STEP 2** Select *Unknown* and click **Go**.

STEP 3 Click **Reset All Unknown Smartports**.

TIP This problem could be a configuration on the interface prior to applying the macro most often encountered with security and storm-control settings, a typo or incorrect command within the user-defined macro, or an invalid parameter setting. Parameters are checked for neither type nor boundary prior to the attempt to apply the macro, therefore, an incorrect or invalid input to a parameter value will almost assuredly cause failure when applying the macro.

Web GUI

The Smartport feature is configured in the *Smartport > Properties*, *Smartport Type Settings* and *Interface Settings* pages.

For Voice VLAN configuration, see the [Voice VLAN](#) section.

For LLDP/CDP configuration, see the [Configuring LLDP](#) and [Configuring CDP](#) sections, respectively.

Properties

To configure the Smartport feature globally:

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

STEP 2 Enter the parameters.

- **Administrative Auto Smartport**—Select to globally enable or disable Auto Smartport. The following options are available:
 - *Disable*—Select to disable Auto Smartport on the device.
 - *Enable*—Select to enable Auto Smartport on the device.
 - *Enable by Voice VLAN*— This enables Auto Smartport but will put it in operation only when Auto Voice VLAN is also enabled and in operation. Enable by Auto Voice VLAN is the default.
- **Operational Auto Smartport Status**—Displays the global status of the Auto Smartport feature.

- **Auto Smartport Device Detection Method**—Select whether incoming CDP, LLDP, or both types of packets are used to detect the Smartport type of the attaching device(s). At least one must be checked in order for Auto Smartport to identify devices.
- **Operational CDP Status**—Displays the operational status of CDP. Enable CDP if Auto Smartport is to detect the Smartport type based on CDP advertisement.
- **Operational LLDP Status**—Displays the operational status of LLDP. Enable LLDP if Auto Smartport is to detect the Smartport type based on LLDP/LLDP-MED advertisement.
- **Auto Smartport Device Detection**—Select each type of device for which Auto Smartport can assign Smartport types to interfaces. If unchecked, Auto Smartport will not assign that Smartport type to any interface.

STEP 3 Click **Apply**. This sets the global Smartport parameters on the switch.

Smartport Type Settings

Use the *Smartport Type Settings* page to edit the Smartport Type settings and view the Macro Source.

By default, each Smartport type is associated with a pair of built-in Smartport macros. See the [Smartport Types](#) page for further information on macro versus anti-macro. Built-in or user-defined macros can have parameters. The built-in macros have up to three parameters.

Editing these parameters for the Smartport types applied by Auto Smartport from the *Smartport Type Settings* page configures the default values for these parameters. These defaults will be used by Auto Smartport.

NOTE Changes to Auto Smartport types will cause the new settings to be applied to interfaces which have already been assigned that type by Auto Smartport. In this case, binding an invalid macro or setting an invalid default parameter value will cause all ports of this Smartport type to become unknown.

STEP 1 Click **Smartport > Smartport Type Settings**. The *Smartport Type Settings* page opens.

STEP 2 To view the Smartport macro associated with a Smartport type, select a Smartport type and click **View Macro Source**.

STEP 3 To modify the parameters of a macro, select a Smartport type and click **Edit**. The *Edit Smartport Type Settings* page opens.

STEP 4 Enter the fields.

- **Port Type**—Select a Smartport type.
- **Macro Name**—Displays the name of the Smartport macro currently associated with the Smartport type.
- **Macro Parameters**—You can restore the default parameter values by clicking **Restore Defaults**.

STEP 5 Click **Apply** to save the changes to the running configuration. If the Smartport macro and/or its parameter values associated with the Smartport type are modified, Auto Smartport will automatically reapply the macro to the interfaces currently assigned with the Smartport type by Auto Smartport. Auto Smartport will not apply the changes to interfaces that were statically assigned a Smartport type.

NOTE There is no method to validate macro parameters because they do not have a type association. Therefore, any entry is valid at this point. However, invalid parameter values may cause errors to occur when the Smartport type is assigned to an interface, applying the associated macro.

Interface Settings

Use the Interface Settings page to perform the following tasks:

- Statically apply a specific Smartport type to an interface with interface specific values for the macro parameters.
- Enable Auto Smartport on an interface.
- Diagnose a Smartport macro which failed upon application, and caused the Smartport type to become unknown.
- Reapply a Smartport macro after it fails on an interface. It is expected that the necessary corrections have been made prior to clicking Reapply. See the workflow area in **Common Smartport Tasks** section for troubleshooting tips.
- Reset unknown interfaces.

- Reapply a Smartport to an interface. In some circumstances, you may want to reapply a Smartport macro so that the configuration at an interface is up to date. For instance, reapplying a switch Smartport macro at a switch interface will make the interface a member of the VLANs created since the last macro application. You have to be familiar with the current configurations on the switch and the definition of the macro to determine if a reapplication has any impact on the interface.

To apply a Smartport macro:

STEP 1 Click **Smartport > Interface Settings**. The *Interface Settings* page opens.

STEP 2 Reapply Smartport Macro by Smartport Types

At the top of the page there is a quick apply for these four interfaces:

- All Switches, Routers, and Wireless Access Points
- All Switches
- All Routers
- All Wireless Access Points

If desired, you can reapply the associated Smartport to all the interfaces that are already assigned with Smartport type switch, router, or wireless Access Points. This step reapplies the macro to all interfaces which have been assigned to the selection in the area at the top of the page called Reapply Smartport Macro:

- **Apply**—Reapply the last macro that was applied to the interface (for certain types listed in screen). This adds the interface to all newly-created VLANs.

STEP 3 Reapply Smartport Macro on selected interfaces. This step allows the user to choose the interface on which to perform the reapplication of the the smartport macro. You do not need to perform both step 2 and step 3.

Select the interface from the Interface Settings Table and click the **Reapply** button. This method is applicable only for interfaces of type Switch, Router, and Wireless Access Points.

STEP 4 Smartport Diagnostic

If a Smartport macro fails, the Smartport Type of the interface is Unknown. Select an interface which is of unknown type and click **Show Diagnostic**. This will show the command at which application of the macro failed. See the workflow area in **Common Smartport Tasks** section for troubleshooting tips. Proceed after correcting the problem.

STEP 5 Select an interface which is of unknown type and click **Edit**. The *Edit Interface Type Settings* page opens. Click **Reset** to reset the interface to default Smartport type before applying/reapplying Auto Smartport or the desired Smartport type to the interface.

STEP 6 Click **Reset All Unknown Smartports** to reset all the interfaces where the Smartport macro has failed. This will return all interfaces to the Default type. After correcting the error in the macro or on the current interface configuration or both, a new macro may be applied.

NOTE Resetting the interface of unknown type does not reset the configuration performed by the macro that failed. This clean up must be done manually.

To assign a Smartport type to an interface or activate Auto Smartport on the interface:

STEP 1 Select an interface and click **Edit**. The *Edit Interface Settings* page opens.

STEP 2 Click **Reset** to reset the interface of an unknown type before applying Auto Smartport or the desired Smartport type to the interface. See the note above.

STEP 3 Enter the fields.

- **Interface**—Select the port or LAG.
- **Smartport Type**—Displays the Smartport type currently assigned to the port/LAG.
- **Smartport Application**—Select the Smartport type from the Smartport Application pull-down.
- **Smartport Application Method**— If Auto Smartport is selected, Auto Smartport will automatically assign the Smartport type based on the CDP and/or LLDP advertisement received from the connecting devices as well as apply corresponding Smartport macro. To statically assign a Smartport type and apply the corresponding Smartport macro to the interface, select the desired Smartport type.
- **Persistent Status**—Select to enable the Persistent status. If enabled, the association of a Smartport type to an interface remains even if the interface goes down, or the switch is rebooted. Persistent is applicable only if the

Smartport Application of the interface is Auto Smartport. Enabling Persistent at an interface eliminates the device detection delay that otherwise will occur.

- **Macro Parameters**—This block displays the parameter values of the Smartport macro applied or to be applied to the interface.
- **Reset**—If an interface is in Unknown status (as a result of an unsuccessful macro application), set it to Default and reapply the last macro that was run on it.

STEP 4 Click **Apply** to update the changes and assign the Smartport type to the interface.

Built-in Smartport Macros

The following describes the pair of built-in macros for each Smartport type. For each Smartport type there is a macro to configure the interface and an anti macro to remove the configuration.

Macro code for the following Smartport types are provided:

- **desktop**
- **printer**
- **guest**
- **server**
- **host**
- **ip_camera**
- **ip_phone**
- **ip_phone_desktop**
- **switch**
- **router**
- **ap**

desktop

```
[desktop]
#interface configuration, for increased network security and reliability when connecting a desktop
device, such as a PC, to a switch port.
#macro description Desktop
#macro keywords $native_vlan $max_hosts
#
#macro key description:  $native_vlan: The untag VLAN which will be configured on the port
#                       $max_hosts: The maximum number of allowed devices on the port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_desktop

```
[no_desktop]
#macro description No Desktop
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

printer

```
[printer]
#macro description printer
#macro keywords $native_vlan
#
#macro key description: $native_vlan: The untag VLAN which will be configured on the port
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_printer

```
[no_printer]
#macro description No printer
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

guest

```
[guest]
#macro description guest
#macro keywords $native_vlan
#
#macro key description: $native_vlan: The untag VLAN which will be configured on the port
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_guest]]

```
[no_guest]
#macro description No guest
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

server

```
[server]
#macro description server
#macro keywords $native_vlan $max_hosts
#
#macro key description: $native_vlan: The untag VLAN which will be configured on the port
#           $max_hosts: The maximum number of allowed devices on the port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```


no_server

```
[no_server]
#macro description No server
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
#
spanning-tree portfast auto
#
@
```

host

```
[host]
#macro description host
#macro keywords $native_vlan $max_hosts
#
#macro key description:  $native_vlan: The untag VLAN which will be configured on the port
#                       $max_hosts: The maximum number of allowed devices on the port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_host

```
[no_host]
#macro description No host
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_camera

```
[ip_camera]
#macro description ip_camera
#macro keywords $native_vlan
#
#macro key description: $native_vlan: The untag VLAN which will be configured on the port
#Default Values are
#$native_vlan = Default VLAN
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_camera

```
[no_ip_camera]
#macro description No ip_camera
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone

```
[ip_phone]
#macro description ip_phone
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:  $native_vlan: The untag VLAN which will be configured on the port
#                       $voice_vlan: The voice VLAN ID
#                       $max_hosts: The maximum number of allowed devices on the port
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone

```
[no_ip_phone]
#macro description no ip_phone
#macro keywords $voice_vlan
#
#macro key description: $voice_vlan: The voice VLAN ID
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone_desktop

```
[ip_phone_desktop]
#macro description ip_phone_desktop
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:  $native_vlan: The untag VLAN which will be configured on the port
#                       $voice_vlan: The voice VLAN ID
#                       $max_hosts: The maximum number of allowed devices on the port
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```


no_ip_phone_desktop

```
[no_ip_phone_desktop]
#macro description no ip_phone_desktop
#macro keywords $voice_vlan
#
#macro key description: $voice_vlan: The voice VLAN ID
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

switch

```
[switch]
#macro description switch
#macro keywords $native_vlan $voice_vlan
#
#macro key description: $native_vlan: The untag VLAN which will be configured on the port
#           $voice_vlan: The voice VLAN ID
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
spanning-tree link-type point-to-point
#
@
```

no_switch

```
[no_switch]
#macro description No switch
#macro keywords $voice_vlan
#
#macro key description: $voice_vlan: The voice VLAN ID
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no spanning-tree link-type
#
@
```

router

```
[router]
#macro description router
#macro keywords $native_vlan $voice_vlan
#
#macro key description: $native_vlan: The untag VLAN which will be configured on the port
#           $voice_vlan: The voice VLAN ID
#
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree link-type point-to-point
#
@
```

no_router

```
[no_router]
#macro description No router
#macro keywords $voice_vlan
#
#macro key description: $voice_vlan: The voice VLAN ID
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
#
no spanning-tree link-type
#
@
```

ap

```
[ap]
#macro description ap
#macro keywords $native_vlan $voice_vlan
#
#macro key description: $native_vlan: The untag VLAN which will be configured on the port
#           $voice_vlan: The voice VLAN ID
#
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
spanning-tree link-type point-to-point
#
@
```

no_ap

```
[no_ap]
#macro description No ap
#macro keywords $voice_vlan
#
#macro key description: $voice_vlan: The voice VLAN ID
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no spanning-tree link-type
#
@
```

Managing Device Diagnostics

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

It includes the following topics:

- [Testing Copper Ports](#)
- [Displaying Optical Module Status](#)
- [Configuring Port and VLAN Mirroring](#)
- [Viewing CPU Utilization and Secure Core Technology](#)

Testing Copper Ports

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

VCT performs two types of tests:

- Time Domain Reflectometry (TDR) technology tests the quality and characteristics of a copper cable attached to a port. Cables of up to 140 meters long can be tested. These results are displayed in the Test Results block of the *Copper Test* page.
- DSP-based tests are performed on active GE links to measure cable length. These results are displayed in the Advanced Information block of the *Copper Test* page.

Preconditions to Running the Copper Port Test

Before running the test, do the following:

- (Mandatory) Disable Short Reach mode (see the Port Management > Green Ethernet > *Properties* page)

- (Optional) Disable EEE (see the Port Management > Green Ethernet > *Properties* page)

Use a CAT5 data cable to run all cable testing (VCT).

Accuracy of the test results can have an error range of +/- 10 for Advanced Testing and +/- 2 for Basic Testing.



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

To test copper cables attached to ports:

- STEP 1** Click **Administration > Diagnostics > Copper Test**. The *Copper Test* page opens.
- STEP 2** Select the port on which to run the test.
- STEP 3** Click **Copper Test**.
- STEP 4** When the message is displayed, click **OK** to confirm that the link can go down or **Cancel** to abort the test.

The following fields are displayed in the Test Results block:

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

If the port being tested is a Giga port, the **Advanced Information block** displays the following information (it is refreshed each time you enter the page):

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

NOTE TDR tests cannot be performed when the port speed is 10Mbit/Sec.

Displaying Optical Module Status

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

MSA-compatible SFPs

MSA-compatible SFPs

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

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

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

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

- MGBLH1: 1000BASE-LH SFP transceiver, for single-mode fiber, 1310 nm wavelength, supports up to 40 km.
- MGBLX1: 1000BASE-LX SFP transceiver, for single-mode fiber, 1310 nm wavelength, supports up to 10 km.
- MGBSX1: 1000BASE-SX SFP transceiver, for multimode fiber, 850 nm wavelength, supports up to 550 m.
- MGBT1: 1000BASE-T SFP transceiver for category 5 copper wire, supports up to 100 m.

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

This page displays the following fields:

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

Configuring Port and VLAN Mirroring

Port mirroring is used on a network switch to send a copy of network packets seen on one switch port, multiple switch ports, or an entire VLAN to a network monitoring connection on another port on the switch. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system. A network analyzer connected to the monitoring port processes the data packets for diagnosing, debugging, and performance monitoring. Up to eight sources can be mirrored. This can be any combination of eight individual ports and/or VLANs.

A packet that is received on a network port assigned to a VLAN that is subject to mirroring, is mirrored to the analyzer port even if the packet was eventually trapped or discarded. Packets sent by the switch are mirrored when Transmit (Tx) mirroring is activated.

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

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

To enable mirroring:

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

This page displays the following fields:

- **Destination Port**—Port to which traffic is to be copied; the analyzer port.
- **Source Interface**—Interface, port, or VLAN, from which traffic is sent to the analyzer port.
- **Type**—Type of monitoring: incoming to the port, outgoing from the port, or both.
- **Status**— Displays one of the following values:
 - *Active*—Both source and destination interfaces are up and forwarding traffic.
 - *Not Ready*—Either source or destination (or both) are down or not forwarding traffic for some reason.

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

STEP 3 Enter the parameters:

- **Destination Port**—Select the analyzer port to where packets are copied. A network analyzer, such as a PC running Wireshark, is connected to this port. If a port is identified as an analyzer destination port, it remains the analyzer destination port until all entries are removed.
- **Source Interface**—Select Port or VLAN as the source port or source VLAN from where traffic is to be mirrored.

- **Type**—Select whether incoming, outgoing, or both types of traffic are mirrored to the analyzer port. If **Port** is selected, the options are:
 - *Rx Only*—Port mirroring on incoming packets.
 - *Tx Only*—Port mirroring on outgoing packets.
 - *Tx and Rx*—Port mirroring on both incoming and outgoing packets.

STEP 4 Click **Apply**. Port mirroring is added, and the Running Configuration file is updated.

Viewing CPU Utilization and Secure Core Technology

This section describes the Secure Core Technology (SCT) and how to view CPU usage.

The switch handles the following types of traffic, in addition to end-user traffic:

- Management traffic
- Protocol traffic
- Snooping traffic

Excessive traffic burdens the CPU, and might prevent normal switch operation.

The switch uses the Secure Core Technology (SCT) feature to ensure that the switch will receive and process management and protocol traffic, no matter how much total traffic is received.

SCT is enabled by default on the device and cannot be disabled.

There are no interactions with other features.

To display CPU utilization:

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

or

STEP 2 Click **Security > Denial of Service Prevention > Security Suite Settings** and click **Details**.

The *CPU Utilization* page opens.

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

STEP 3 Select **CPU Utilization** to enable viewing CPU resource utilization information.

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

STEP 4 Select the **Refresh Rate** (time period in seconds) that passes before the statistics are refreshed. A new sample is created for each time period.

Managing Power-over-Ethernet Devices

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

This section describes how to use the PoE feature.

It includes the following topics:

- [PoE on the Switch](#)
- [Configuring PoE Properties](#)
- [Configuring the PoE Power, Priority, and Class](#)

PoE on the Switch

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

PoE Features

PoE Features

PoE provides the following features:

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

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

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

PoE Operation

PoE Operation

PoE implements in the following stages:

- **Detection**—Sends special pulses on the copper cable. When a PoE device is located at the other end, that device responds to these pulses.
- **Classification**—Negotiation between the Power Sourcing Equipment (PSE) and the Powered Device (PD) commences after the Detection stage. During negotiation, the PD specifies its class, which is the amount of maximum power that the PD consumes.
- **Power Consumption**—After the classification stage completes, the PSE provides power to the PD. If the PD supports PoE, but without classification, it is assumed to be class 0 (the maximum). If a PD tries to consume more power than permitted by the standard, the PSE stops supplying power to the port.

PoE supports two modes:

- **Port Limit**—The maximum power the switch agrees to supply is limited to the value the system administrator configures, regardless of the Classification result.
- **Class Power Limit**—The maximum power the switch agrees to supply is determined by the results of the Classification stage. This means that it is set as per the Client's request.

PoE Configuration Considerations

PoE Configuration Considerations

There are two factors to consider in the PoE feature:

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

You can decide the following:

- Maximum power a PSE is allowed to supply to a PD
- During device operation, to change the mode from Class Power Limit to Port Limit and vice versa. The power values per port that were configured for the Port Limit mode are retained.
- Maximum port limit allowed as a per-port numerical limit in mW (Port Limit mode).
- To generate a trap when a PD tries to consume too much and at what percent of the maximum power this trap is generated.

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

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

- Maintains the up/down status of the PoE port link
- Turns off power delivery to the PoE port
- Logs the reason for turning off power
- Generates a trap to a remote log server

Configuring PoE Properties

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

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

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

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

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

STEP 2 Enter the values for the following fields:

- **Power Mode**—Select one of the following options:
 - *Port Limit*—The maximum power limit per each port is configured by the user.
 - *Class Limit*—The maximum power limit per port is determined by the class of the device, which results from the Classification stage.
- **Traps**—Enable or disable a SYSLOG trap.
- **Power Trap Threshold**—Enter the usage threshold that is a percentage of the power limit. An alarm is initiated if the power exceeds this value.

The following counters are displayed:

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

STEP 3 Click **Apply** to save the PoE properties.

Configuring the PoE Power, Priority, and Class

The *PoE Settings* page displays system PoE information for enabling PoE on the interfaces and monitoring the current power usage and maximum power limit per port.

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

- **Port Limit:** Power is limited to a specified wattage. For these settings to be active, the system must be in PoE Port Limit mode. That mode is configured in the *PoE Properties* page.

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

- **Class Limit:** Power is limited based on the class of the connected PD. For these settings to be active, the system must be in PoE Class Limit mode. That mode is configured in the *PoE Properties* page.

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

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

See the [Smart Switch Models](#) table for a description of the switch models that support PoE and the maximum power that can be allocated to PoE ports.

To configure PoE port settings:

-
- STEP 1** Click **Port Management > PoE > Settings (Port Limit)**. The *PoE Settings* page opens.
 - STEP 2** Select a port and click **Edit**. The *Edit PoE Settings* page opens.
 - STEP 3** Enter the value for the following field:
 - **Interface**—Select the port to configure.
 - **PoE Administrative Status**—Enable or disable PoE on the port.

- **Power Priority Level**—Select the port priority: low, high, or critical, for use when the power supply is low. For example, if the power supply is running at 99% usage and port 1 is prioritized as high, but port 3 is prioritized as low, port 1 receives power and port 3 might be denied power.
- **Administrative Power Allocation**—This field is displayed only if the Power Mode set in the PoE Properties page is Port Limit. If the Power mode is Power Limit, enter the power in milliwatts allocated to the port. The range is 0 to 15,400.
- **Max Power Allocation**—Displays the maximum amount of power permitted on this port.
- **Class**—This field is displayed only if the Power Mode set in the *PoE Properties* page is Class Limit. The class determines the power level:

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

- **Power Consumption**—Displays the amount of power in milliwatts assigned to the powered device connected to the selected interface.
- **Overload Counter**—Displays the total number of power overload occurrences.
- **Short Counter**—Displays the total number of power shortage occurrences.
- **Denied Counter**—Displays number of times the powered device was denied power.
- **Absent Counter**—Displays the number of times that power was stopped to the powered device, because the powered device was no longer detected.
- **Invalid Signature Counter**—Displays the times an invalid signature was received. Signatures are the means by which the powered device identifies itself to the PSE. Signatures are generated during powered device detection, classification, or maintenance.

- STEP 4** Click **Apply**. The PoE settings for the port are defined and the Running Configuration file is updated.
-

VLAN Management

This section contains the following topics:

- **VLANs**
- **Configuring Default VLAN Settings**
- **Creating VLANs**
- **Configuring VLAN Interface Settings**
- **Defining VLAN Membership**
- **Voice VLAN**

VLANs

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

VLAN Description

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

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

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

If a frame is VLAN-tagged, a four-byte VLAN tag is added to each Ethernet frame, increasing the maximum frame size from 1518 to 1522. The tag contains a VLAN ID between 1 and 4094, and a VLAN Priority Tag (VPT) between 0 and 7. See *QoS Operation* for details about VPT.

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

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

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

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

The egress port:

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

VLAN Roles

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

Device VLANs can only be created statically.

Some VLANs can have additional roles, including:

- Voice VLAN: For more information refer to the *Voice VLAN* section.
- Guest VLAN: Set in the *Edit VLAN Authentication* page.
- Default VLAN: For more information refer to the *Configuring Default VLAN Settings* section.

- **Management VLAN:** For more information refer to the *Configuring IP Information* section.

QinQ

QinQ provides isolation between service provider networks and customers' networks. The switch is a provider bridge that supports port-based c-tagged service interface.

With QinQ, the switch adds an ID tag known as Service Tag (S-tag) to forward traffic over the network. The S-tag is used to segregate traffic between various customers, while preserving the customer VLAN tags.

Customer traffic is encapsulated with an S-tag with TPID 0x8100, regardless of whether it was originally c-tagged or untagged. The S-tag allows this traffic to be treated as an aggregate within a provider bridge network, where the bridging is based on the S-tag VID (S-VID) only.

The S-Tag is preserved while traffic is forwarded through the network service provider's infrastructure, and is later removed by an egress device.

An additional benefit of QinQ is that there is no need to configure customers' edge devices.

QinQ is enabled in the VLAN Management > *Interface Settings* page.

VLAN Configuration Workflow

To configure VLANs:

1. If required, change the default VLAN by using the [Configuring Default VLAN Settings](#) section.
2. Create the required VLANs by using the [Creating VLANs](#) section.
3. Set the desired VLAN-related configuration for ports and enable QinQ on an interface using the [Configuring VLAN Interface Settings](#) section.
4. Assign interfaces to VLANs by using the [Configuring Port to VLAN](#) section or the [Configuring VLAN Membership](#) section.
5. View the current VLAN port membership for all the interfaces in the [Configuring VLAN Membership](#) section.

Configuring Default VLAN Settings

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

The default VLAN has the following characteristics:

- It is distinct, non-static/non-dynamic, and all ports are untagged members by default.
- It cannot be deleted.
- It cannot be given a label.
- It cannot be used for any special role, such as unauthenticated VLAN or Voice VLAN.
- If a port is no longer a member of any VLAN, the switch automatically configures the port as an untagged member of the default VLAN. A port is no longer a member of a VLAN if the VLAN is deleted or the port is removed from the VLAN.

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

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

To change the default VLAN:

- STEP 1** Click **VLAN Management > Default VLAN Settings**. The *Default VLAN Settings* page opens.
- STEP 2** Enter the value for the following field:
 - **Current Default VLAN ID**—Displays the current default VLAN ID.
 - **Default VLAN ID After Reboot**—Enter a new VLAN ID to replace the default VLAN ID after reboot.
- STEP 3** Click **Apply**.
- STEP 4** Click **Save** (in the upper-right corner of the window) and save the Running Configuration to the Startup Configuration.

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

Creating VLANs

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

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

Each VLAN must be configured with a unique VID (VLAN ID) with a value from 1 to 4094. The switch reserves VID 4095 as the Discard VLAN. All packets classified to the Discard VLAN are discarded at ingress, and are not forwarded to a port.

To create a VLAN:

STEP 1 Click **VLAN Management > Create VLAN**. The *Create VLAN* page opens.

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

- **VLAN ID**—User-defined VLAN ID.
- **VLAN Name**—User-defined VLAN name.
- **Type**—VLAN type:
 - *Static*—VLAN is user-defined.
 - *Default*—VLAN is the default VLAN.

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

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

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

To create a range of VLANs, select the **Range** radio button, and specify the range of VLANs to be created by entering the Starting VID and Ending VID, inclusive. When using the **Range** function, the maximum number of VLANs you can create at one time is 100.

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

Configuring VLAN Interface Settings

The *Interface Settings* page displays and enables configuration of VLAN-related parameters for all interfaces.

To configure the VLAN settings:

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

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

STEP 3 To configure a Port or LAG, select it and click **Edit**. The *Edit Interface Setting* page opens.

STEP 4 Enter the values for the following fields:

- **Interface**—Select a Port/LAG.
- **Interface VLAN Mode**—Select the interface mode for the VLAN. The options are:
 - *General*—The interface can support all functions as defined in the IEEE 802.1q specification. The interface can be a tagged or untagged member of one or more VLANs.
 - *Access*—The interface is an untagged member of a single VLAN. A port configured in this mode is known as an access port.
 - *Trunk*—The interface is an untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. A port configured in this mode is known as a trunk port.
 - *Customer*—Selecting this option places the interface in QinQ mode. This enables the user to use their own VLAN arrangements (PVID) across the provider network. The switch will be in Q-in-Q mode when it has one or more customer ports. See [QinQ](#).
- **Administrative PVID**—Enter the Port VLAN ID (PVID) of the VLAN to which incoming untagged and priority tagged frames are classified. The possible values are 1 to 4094.
- **Frame Type**—Select the type of frame that the interface can receive. Frames that are not of the configured frame type are discarded at ingress. These frame types are only available in General mode. Possible values are:
 - *Admit All*—The interface accepts all types of frames: untagged frames, tagged frames, and priority tagged frames.
 - *Admit Tagged Only*—The interface accepts only tagged frames.
 - *Admit Untagged Only*—The interface accepts only untagged and priority frames.
- **Ingress Filtering**—(Available only in General mode) Select to enable ingress filtering. When an interface is ingress filtering enabled, the interface discards all incoming frames that are classified as VLANs of which the interface is not a member. Ingress filtering can be disabled or enabled on general ports. It is always enabled on access ports and trunk ports.

STEP 5 Click **Apply**. The parameters are written to the Running Configuration file.

Defining VLAN Membership

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

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

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

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

VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices. If a destination end node is VLAN-unaware, but is to receive traffic from a VLAN, then the last VLAN-aware device (if there is one), must send frames of the destination VLAN to the end node untagged. That is, the egress port that reaches the end node must be an untagged member of the VLAN.

Configuring Port to VLAN

Use the *Port to VLAN* page to display and configure the ports within a specific VLAN.

To map ports or LAGs to a VLAN:

-
- STEP 1** Click **VLAN Management > Port to VLAN**. The *Port to VLAN* page opens.
 - STEP 2** Select a VLAN and the interface type (Port or LAG), and click **Go** to display or to change the port characteristic with respect to the VLAN.

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

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

- STEP 3** Change the registration of an interface to the VLAN by selecting the desired option from the following list:
- **Forbidden**—The interface is not allowed to join the VLAN. When a port is not a member of any other VLAN, enabling this option on the port makes the port part of internal VLAN 4095 (a reserved VID).
 - **Excluded**—The interface is currently not a member of the VLAN. This is the default for all the ports and LAGs when the VLAN is newly created.
 - **Tagged**—The interface is a tagged member of the VLAN.
 - **Untagged**—The interface is an untagged member of the VLAN. Frames of the VLAN are sent untagged to the interface VLAN.
 - **PVID**—Select to set the PVID of the interface to the VID of the VLAN. PVID is a per-port setting.
- STEP 4** Click **Apply**. The interfaces are assigned to the VLAN, and written to the Running Configuration file.

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

Configuring VLAN Membership

The *Port VLAN Membership* page displays all ports on the device along with a list of VLANs to which each port belongs.

If the port-based authentication method for an interface is 802.1x and the Administrative Port Control is Auto, then:

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

To assign a port to one or more VLANs:

-
- STEP 1** Click **VLAN Management > Port VLAN Membership**. The *Port VLAN Membership* page opens.
- STEP 2** Select interface type (Port or LAG), and click **Go**. The following fields are displayed for all interfaces of the selected type:
- **Interface**—Port/LAG ID.
 - **Mode**—Interface VLAN mode that was selected in the *Interface Settings* page.
 - **Administrative VLANs**—Drop-down list that displays all VLANs of which the interface might be a member.
 - **Operational VLANs**—Drop-down list that displays all VLANs of which the interface is currently a member.
 - **LAG**—If interface selected is Port, displays the LAG in which it is a member.
- STEP 3** Select a port, and click the **Join VLAN** button. The *Join VLAN To Port* page opens.
- STEP 4** Enter the values for the following fields:
- **Interface**—Select a Port or LAG.
 - **Mode**—Displays the port VLAN mode that was selected in the *Interface Settings* page.
 - **Select VLAN**—To associate a port with a VLAN(s), move the VLAN ID(s) from the left list to the right list by using the arrow buttons. The default VLAN might appear in the right list if it is tagged, but it cannot be selected.
 - **Tagging**—Select one of the following tagging/PVID options:
 - **Forbidden**—The interface is not allowed to join the VLAN. When a port is not a member of any other VLAN, enabling this option on the port makes the port part of internal VLAN 4095 (a reserved VID).
 - **Excluded**—The interface is currently not a member of the VLAN. This is the default for all the ports and LAGs when the VLAN is newly created.
 - **Tagged**—Select whether the port is tagged. This is not relevant for Access ports.
 - **Untagged**—Select whether port is untagged. This is not relevant for Access ports.

- **PVID**—Port PVID is set to this VLAN. If the interface is in access mode or trunk mode, the switch automatically makes the interface an untagged member of the VLAN. If the interface is in general mode, you must manually configure VLAN membership.

STEP 5 Click **Apply**. The settings are modified and written to the Running Configuration file.

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

Voice VLAN

In a LAN, voice devices, such as IP phones, VoIP endpoints, and voice systems are placed into the same VLAN. This VLAN is referred to as the voice VLAN. If the voice devices are in different voice VLANs, IP (L3) routers are needed to provide communication.

It contains the following topics:

- [Voice VLAN Overview](#)
- [Configuring Voice VLAN](#)

Voice VLAN Overview

This section contains the following topics:

- [Dynamic Voice VLAN Modes](#)
- [Auto Voice VLAN, Auto Smartports, CDP, and LLDP](#)
- [Voice VLAN QoS](#)
- [Voice VLAN Constraints](#)
- [Voice VLAN Workflows](#)

The following are typical voice deployment scenarios with appropriate configurations:

- **UC3xx/UC5xx hosted:** All Cisco phones and VoIP endpoints support this deployment model. For this model, the UC3xx/UC5xx, Cisco phones and VoIP endpoints reside in the same voice VLAN. The voice VLAN of UC3xx/UC5xx defaults to VLAN 100.
- **Third party IP PBX-hosted:** Cisco SBTG CP-79xx, SPA5xx phones and SPA8800 endpoints support this deployment model. In this model, the VLAN used by the phones is determined by the network configuration. There may or may not be separate voice and data VLANs. The phones and VoIP endpoints register with an on-premise IP PBX.
- **IP Centrex/ITSP hosted:** Cisco CP-79xx, SPA5xx phones and SPA8800 endpoints support this deployment model. For this model, the VLAN used by the phones is determined by the network configuration. There may or may not be separate voice and data VLANs. The phones and VoIP endpoints register with an off-premise SIP proxy in “the cloud”.

From a VLAN perspective, the above models operate in both VLAN-aware and VLAN-unaware environments. In the VLAN-aware environment, the voice VLAN is one of the many VLANs configured in an installation. The VLAN-unaware scenario is equivalent to a VLAN-aware environment with only one VLAN.

The switch always operates as a VLAN-aware switch.

The switch supports a single voice VLAN. The voice VLAN is defaulted to VLAN 1. A different voice VLAN can be manually configured. It can also be dynamically learned when Auto Voice VLAN is enabled.

Ports can be manually added to the voice VLAN by using basic VLAN configuration as described in the *Configuring VLAN Interface Setting* section, or by manually applying voice related Smartport macro to the ports. Alternatively, they can be added dynamically if the switch is in Telephony OUI mode, or has Auto Smartports enabled.

Dynamic Voice VLAN Modes

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

- **Telephony OUI**

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

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

- **Auto Voice VLAN**

In Auto Voice VLAN mode, the voice VLAN can be either the default voice VLAN, manually configured, or learned from external devices such as UC3xx/5xx and from switches that advertise voice VLAN in CDP or VSDP. VSDP is a Cisco Small Business defined protocol for voice service discovery.

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

Voice End-Points

To have a voice VLAN work properly, the voice devices, such as Ciscos phones and VoIP endpoints, must be assigned to the voice VLAN where it sends and receives its voice traffic. Some of the possible scenarios are as follows:

- A phone/endpoint may be statically configured with the voice VLAN.
- A phone/endpoint may obtain the voice VLAN in the boot file it downloads from a TFTP server. A DHCP server may specify the boot file and the TFTP server when it assigns an IP address to the phone.
- A phone/endpoint may obtain the voice VLAN information from CDP and LLDP-MED advertisements it receives from their neighbor voice systems and switches.

The switch expects the attaching voice devices to send voice VLAN, tagged packets. On ports where the voice VLAN is also the native VLAN, voice VLAN untagged packets are possible.

Auto Voice VLAN, Auto Smartports, CDP, and LLDP

Defaults

By factory defaults, CDP, LLDP, and LLDP-MED on the switch are enabled, auto Smartport mode is enabled, Basic QoS with trusted DSCP is enabled, and all ports are members of default VLAN 1, which is also the default Voice VLAN.

In addition, Dynamic Voice VLAN mode is the default to Auto Voice VLAN with enabling based on trigger, and Auto Smartport is the default to be enabled depending on Auto Voice VLAN.

Voice VLAN Triggers

When Dynamic Voice VLAN mode is Auto Voice VLAN enabled based on trigger, it means Auto Voice VLAN will become operational only if one or more triggers occur. Possible triggers are static voice VLAN configuration, voice VLAN information received in neighbor CDP advertisement, and voice VLAN information received in Voice VLAN Discovery Protocol (VSDP). If desired, an administrator can make Auto Voice VLAN mode operate immediately without waiting for a trigger.

When Auto Smartport is enabled depending on Auto Voice VLAN mode, it means Auto Smartport will be enabled when Auto Voice VLAN becomes operational. If desired, an administrator can enable Auto Smartport independent of Auto Voice VLAN.

NOTE The default configuration list here applies to switches whose firmware version supports Auto Voice VLAN out of the box. It also applies to unconfigured switches that have been upgraded to the firmware version that supports Auto Voice VLAN.

NOTE The defaults and the voice VLAN triggers are designed to have no effect on any installations without a voice VLAN and on switches that have already been configured. You may manually disable and enable Auto Voice VLAN and/or Auto Smartport to fit your deployment if needed.

Auto Voice VLAN

Auto Voice VLAN is responsible to maintain the voice VLAN, but depends on Auto Smartport to maintain the voice VLAN port memberships. Auto Voice VLAN performs the following functions when it is in operation:

- It discovers voice VLAN information in CDP advertisements from directly connected neighbor devices.
- If multiple neighbor switches and/or routers, such as Cisco UC devices, are advertising their voice VLAN, the voice VLAN from the device with the lowest MAC address is used.

NOTE If connecting the switch to a Cisco UC device, you may need to configure the port on the UC device using the `switchport voice vlan` command to ensure the UC device advertises its voice VLAN in CDP at the port.

- It synchronizes the voice VLAN-related parameters with other Auto Voice VLAN-enabled switches, using Voice Service Discovery Protocol (VSDP). The switch always configures itself with the voice VLAN from the highest priority source it is aware of. The priority is based on the source type and MAC address of the source providing the voice VLAN information. Source type priority from high to low are static VLAN configuration, CDP advertisement, and default configuration based on changed default VLAN, and default voice VLAN. A numeric low MAC address is of higher priority than a numeric high MAC address.
- It maintains the voice VLAN until a new voice VLAN from a higher priority source is discovered or until the Auto Voice VLAN is restarted by the administrator. When restarted, the switch resets the voice VLAN to the default voice VLAN and restarts the Auto Voice VLAN discovery.
- When a new voice VLAN is configured/discovered, the switch automatically creates it, and replaces all the port memberships of the existing voice VLAN to the new voice VLAN. This may interrupt or terminate existing voice sessions, which is expected when network topology is altered.

NOTE If the switch is in Layer 2 mode, it can synchronize with only VSDP capable switches in the same management VLAN. If the switch is in layer 3 mode, it can synchronize with VSDP capable switches that are in the directly-connected IP subnets configured at the switch.

Auto Smartport works with CDP/LLDP to maintain the port memberships of the voice VLAN when voice end-points are detected from the ports:

- When CDP and LLDP are enabled, the switch sends out CDP and LLDP packets periodically to advertise the voice VLAN to the voice endpoints to use.
- When a device attaching to a port advertises itself as a voice endpoint through CDP and/or LLDP, the Auto Smartport automatically adds the port to the voice VLAN by applying the corresponding Smartport macro to the port (if there is no other devices from the port advertising a conflicting or superior capability). If a device advertises itself as a phone, the default Smartport macro is phone. If a device advertises itself as a phone and host or phone and bridge, the default Smartport macro is phone+desktop.

Voice VLAN QoS

Voice VLAN can propagate the CoS/802.1p and DSCP settings by using LLDP-MED Network policies. The LLDP-MED is set by default to respond with the Voice QoS setting if an appliance sends LLDP-MED packets. MED-supported devices should send their voice traffic with the same CoS/802.1p and DSCP values, as received with the LLDP-MED response.

The user can disable the automatic update between Voice VLAN and LLDP-MED and use his own network policies.

Working with the OUI mode, the switch can additionally configure the mapping and remarking (CoS/802.1p) of the voice traffic based on the OUI.

By default, all interfaces are CoS/802.1p trusted. The switch applies the quality of service based on the CoS/802.1p value found in the voice stream. For Telephony OUI voice streams, the user can override the quality of service and optionally remark the 802.1p of the voice streams by specifying the desired CoS/802.1p values and using the remarking option under Telephony OUI.

Voice VLAN Constraints

The following constraints exist:

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

In addition the following constraints are applicable for Telephony OUI:

- The Voice VLAN cannot be VLAN1 (the default VLAN).
- The Voice VLAN cannot be Smartport enabled.
- A new VLAN ID can be configured for the Voice VLAN only if the current Voice VLAN does not have candidate ports.
- The interface VLAN of a candidate port must be in General or Trunk mode.
- The Voice VLAN QoS decision has priority over any other QoS decision, except for the Policy decision.
- The Voice VLAN QoS is applied to candidate ports that have joined the Voice VLAN, and to static ports.
- The voice flow is accepted if the MAC address can be learned by the Forwarding Database (FDB). (If there is no free space in FDB, no action occurs).

Voice VLAN Workflows

The switch default configuration on Auto Voice VLAN, Auto Smartports, CDP, and LLDP cover most common voice deployment scenarios. This section describes how to deploy voice VLAN when the default configuration does not apply.

Workflow1: To configure Auto Voice VLAN:

-
- STEP 1** Open the *VLAN Management > Voice VLAN > Properties* page.
 - STEP 2** Select the Voice VLAN ID. It cannot be set to VLAN ID 1 (this step is not required for dynamic Voice VLAN).
 - STEP 3** Set **Dynamic Voice VLAN** to Enable Auto Voice VLAN.
 - STEP 4** Select the **Auto Voice VLAN Activation** method.
 - NOTE** If the device is currently in Telephony OUI mode, you must disable it before you can configure Auto Voice Vlan
 - STEP 5** Click **Apply**.
 - STEP 6** Configure Smartports as described in the **Common Smartport Tasks** section.
 - STEP 7** Configure LLDP/CDP as described in the **Configuring LLDP** and **Configuring CDP** sections, respectively.
 - STEP 8** Enable the Smartport feature on the relevant ports using the *Smartport > Interface Settings* page.

Workflow2: To configure the Telephony OUI Method

-
- STEP 1** Open the *VLAN Management > Voice VLAN > Properties* page. Set **Dynamic Voice VLAN** to Enable Telephony OUI.
 - NOTE** If the device is currently in Auto Voice VLAN mode, you must disable it before you can enable Telephony OUI.
 - STEP 2** Configure Telephony OUI in the *Telephony OUI* page.
 - STEP 3** Configure Telephony OUI VLAN membership for ports in the *Telephony OUI Interface* page.

Configuring Voice VLAN

This section describes how to configure voice VLAN. It contains the following topics:

- **Configuring Voice VLAN Properties**
- **Displaying Auto Voice VLAN Settings**
- **Configuring Telephony OUI**

Configuring Voice VLAN Properties

Use the *Voice VLAN Properties* page for the following:

- View how voice VLAN is currently configured.
- Configure the VLAN ID of the Voice VLAN.
- Configure voice VLAN QoS settings.
- Configure the voice VLAN mode (Telephony OUI or Auto Voice VLAN).
- Configure how Auto Voice VLAN is triggered.

To view and configure Voice VLAN properties:

-
- STEP 1** Click **VLAN Management > Voice VLAN > Properties**. The *Properties* page opens.
- The voice VLAN settings configured on the switch are displayed in the **Voice VLAN Settings (Administrative Status)** block.
 - The voice VLAN settings that are actually being applied to the voice VLAN deployment are displayed in the **Voice VLAN Settings (Operational Status)** block.
- STEP 2** Enter values for the following fields:
- **Voice VLAN ID**—Enter the VLAN that is to be the Voice VLAN.
NOTE Changes in the voice VLAN ID, CoS/802.1p, and/or DSCP will cause the switch to advertise the administrative voice VLAN as a static voice VLAN. If the option *Auto Voice VLAN Activation* triggered by external Voice VLAN is selected, then the default values need to be maintained.
 - **CoS/802.1p**—Select a CoS/802.1p value that will be used by LLDP-MED as a voice network policy. Refer to *Administration > Discovery > LLDP > LLDP MED Network Policy* for additional details.
 - **DSCP**—Selection of DSCP values that will be used by the LLDP-MED as a voice network policy. Refer to *Administration > Discovery > LLDP > LLDP MED Network Policy* for additional details.

- **Dynamic Voice VLAN**—Select this field to disable or enable voice VLAN feature in one of the following ways:
 - *Enable Auto Voice VLAN*—Enable Dynamic Voice VLAN in Auto Voice VLAN mode.
 - *Enable Telephony OUI*—Enable Dynamic Voice VLAN in Telephony OUI mode.
 - *Disable*—Disable Auto Voice Vlan or Telephony OUI.
- **Auto Voice VLAN Activation**—If Auto Voice VLAN was enabled, select one of the following options to activate Auto Voice VLAN:
 - *Immediate*—Auto Voice VLAN on the switch is to be activated and put into operation immediately if enabled.
 - *By External Voice VLAN Trigger*—Auto Voice VLAN on the switch is activated and put into operation only if the switch detects a device advertising the voice VLAN.

NOTE Manually re-configuring the voice VLAN ID, CoS/802.1p, and/or DSCP from their default values will result in a static voice VLAN, which has higher priority than auto voice VLAN that was learned from external sources.

STEP 3 Click **Apply**. The VLAN properties are written to the Running Configuration file.

Displaying Auto Voice VLAN Settings

If Auto Voice VLAN mode is enabled, use the Auto Voice VLAN page to view the relevant global and interface parameters.

You can also use this page to manually restart Auto Voice VLAN, by clicking **Restart Auto Voice VLAN**. After a short delay, this resets the voice VLAN to the default voice VLAN and restarts the Auto Voice VLAN discovery and synchronization process on all the switches in the LAN that are Auto Voice VLAN enabled.

NOTE This will only reset the voice VLAN to the default voice vlan if the Source Type is in the *Inactive* state.

To view Auto Voice VLAN parameters:

- STEP 1** Click **VLAN Management > Voice VLAN > Auto Voice VLAN**. The *Auto Voice VLAN* page opens.

The operation status block on this page shows the information about the current voice VLAN and its source:

- **Auto Voice VLAN Status**—Displays whether Auto Voice VLAN is enabled.
 - **Voice VLAN ID**—The identifier of the current voice VLAN
 - **Source Type**—Displays the type of source where the voice VLAN is discovered by the root switch.
 - **CoS/802.1p**—Displays CoS/802.1p values that will be used by the LLDP-MED as a voice network policy.
 - **DSCP**—Displays DSCP values that will be used by the LLDP-MED as a voice network policy.
 - **Root Switch MAC Address**—The MAC address of the Auto Voice VLAN root device that discovers or is configured with the voice VLAN from which the voice VLAN is learned.
 - **Switch MAC Address**—Base MAC address of the switch. If the device's Switch MAC address is the Root Switch MAC Address, the device is the Auto Voice VLAN root device.
 - **Voice VLAN ID Change Time**—Last time that voice VLAN was updated.
- STEP 2** Click **Restart Auto Voice VLAN** to reset the voice VLAN to the default voice VLAN and restart Auto Voice VLAN discovery on all the Auto-Voice-VLAN-enabled switches in the LAN.

The Voice VLAN Local Table contains local voice VLAN configuration as well as any voice VLAN configuration advertised by directly connected neighbor devices:

For each port the **Best Local Source** is indicated, as follows:

- **Yes**—The switch uses this voice VLAN to synchronize with other Auto Voice VLAN-enabled switches. This voice VLAN will be the voice VLAN for the network unless a voice VLAN from a higher priority source is discovered. Only one local source is the best local source.
- **No**—This is not the best local source.

STEP 3 Click **Refresh** to refresh the information on the page

Configuring Telephony OUI

OUIs are assigned by the Institute of Electrical and Electronics Engineers, Incorporated (IEEE) Registration Authority. Since the number of IP phone manufacturers is limited and well-known, the known OUI values cause the relevant frames, and the port on which they are seen, to be automatically assigned to a Voice VLAN.

The OUI Global table can hold up to 128 OUIs.

This section contains the following topics:

- **Adding OUIs to the Telephony OUI Table**
- **Adding Interfaces to Voice VLAN on Basis of OUIs**

Adding OUIs to the Telephony OUI Table

Use the *Telephony OUI* page to configure Telephony OUI QoS properties. In addition, the Auto Membership Aging time can be configured. If the specified time period passes with no telephony activity, the port is removed from the Voice VLAN.

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

To configure Telephony OUI and/or add a new Voice VLAN OUI:

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

The *Telephony OUI* page displays the following fields:

- **Telephony OUI Operational Status**—Displays whether OUIs are used to identify voice traffic.
- **CoS/802.1p**—Select the CoS queue to be assigned to voice traffic.
- **Remark CoS/802.1p**—Select whether to remark egress traffic.
- **Auto Membership Aging Time**—Enter the time delay to remove a port from the voice VLAN after all of the MAC addresses of the phones detected on the ports have aged out.

STEP 2 Click **Apply** to update the Running Configuration of the switch with these values.

The Telephony OUI table is displayed:

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

STEP 3 Click **Restore OUI Defaults** to delete all of the user-created OUIs, and leave only the default OUIs in the table.

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

STEP 4 To add a new OUI, click **Add**. The *Add Telephony OUI* page opens.

STEP 5 Enter the values for the following fields:

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

STEP 6 Click **Apply**. The OUI is added to the Telephony OUI Table.

Adding Interfaces to Voice VLAN on Basis of OUIs

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

- **All**—Quality of Service (QoS) values configured to the Voice VLAN are applied to all of the incoming frames that are received on the interface and are classified to the Voice VLAN.
- **Telephony Source MAC Address (SRC)**—The QoS values configured for the Voice VLAN are applied to any incoming frame that is classified to the Voice VLAN and contains an OUI in the source MAC address that matches a configured telephony OUI.

Use the *Telephony OUI Interface* page to add an interface to the voice VLAN on the basis of the OUI identifier and to configure the OUI QoS mode of voice VLAN.

To configure Telephony OUI on an interface:

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

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

STEP 2 To configure an interface to be a candidate port of the telephony OUI-based voice VLAN, click **Edit**. The *Edit Interface Settings* page opens.

STEP 3 Enter the values for the following fields:

- **Interface**—Select an interface.
- **Telephony OUI VLAN Membership**—If enabled, the interface is a candidate port of the telephony OUI based voice VLAN. When packets that match one of the configured telephony OUI are received, the port is added to the voice VLAN.
- **Voice VLAN QoS Mode**—Select one of the following options:
 - *All*—QoS attributes are applied only on all packets that are classified to the Voice VLAN.
 - *Telephony Source MAC Address*—QoS attributes are applied only on packets from IP phones.

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

Configuring the Spanning Tree Protocol

The Spanning Tree Protocol (STP) (IEEE802.1D and IEEE802.1Q) is enabled by default, set to RSTP (Rapid Spanning Tree Protocol) mode, and protects a Layer 2 Broadcast domain from broadcast storms by selectively setting links to standby mode to prevent loops. In standby mode, these links temporarily do not transfer user data. They are automatically re-activated when the topology changes to make it desirable to transfer user data.

This section contains the following topics:

- [STP Flavors](#)
- [Configuring STP Status and Global Settings](#)
- [Defining Spanning Tree Interface Settings](#)
- [Configuring Rapid Spanning Tree Settings](#)

STP Flavors

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

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

The switch supports the following Spanning Tree Protocol versions:

- Classic STP provides a single path between any two end stations, avoiding and eliminating loops.
- Rapid STP (RSTP) detects network topologies to provide faster convergence of the spanning tree. This is most effective when the network

topology is naturally tree-structured, and therefore faster convergence might be possible. RSTP is enabled by default.

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

NOTE The 200 Series switches do not support MSTP.

Configuring STP Status and Global Settings

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

Use the *STP Interface Settings* page and *RSTP Interface Settings* page to configure ports with these modes, respectively.

To set STP status and global settings:

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

STEP 2 Enter the parameters.

Global Settings:

- **Spanning Tree State**—Enable or disable STP on the switch.
- **STP Operation Mode**—Select an STP mode.
- **BPDU Handling**—Select how Bridge Protocol Data Unit (BPDU) packets are managed when STP is disabled on the port or the switch. BPDUs are used to transmit spanning tree information.
 - *Filtering*—Filters BPDU packets when Spanning Tree is disabled on an interface.
 - *Flooding*—Floods BPDU packets when Spanning Tree is disabled on an interface.
- **Path Cost Default Values**—Selects the method used to assign default path costs to the STP ports. The default path cost assigned to an interface varies according to the selected method.
 - *Short*—Specifies the range 1 through 65,535 for port path costs.

- *Long*—Specifies the range 1 through 200,000,000 for port path costs.

Bridge Settings:

- **Priority**—Sets the bridge priority value. After exchanging BPDUs, the device with the lowest priority becomes the Root Bridge. In the case that all bridges use the same priority, then their MAC addresses are used to determine which is the Root Bridge. The bridge priority value is provided in increments of 4096. For example, 4096, 8192, 12288, and so on.
- **Hello Time**—Set the interval in seconds that a Root Bridge waits between configuration messages. The range is 1 to 10 seconds.
- **Max Age**—Set the interval in seconds that the switch can wait without receiving a configuration message, before attempting to redefine its own configuration.
- **Forward Delay**—Set the interval in seconds that a bridge remains in a learning state before forwarding packets. For more information, refer to *Defining Spanning Tree Interface Settings*.

Designated Root:

- **Bridge ID**—The bridge priority concatenated with the MAC address of the switch.
- **Root Bridge ID**—The Root Bridge priority concatenated with the MAC address of the Root Bridge.
- **Root Port**—The port that offers the lowest cost path from this bridge to the Root Bridge. (This is significant when the bridge is not the root.)
- **Root Path Cost**—The cost of the path from this bridge to the root.
- **Topology Changes Counts**—The total number of STP topology changes that have occurred.
- **Last Topology Change**—The time interval that elapsed since the last topology change occurred. The time is displayed in a days/hours/minutes/seconds format.

STEP 3 Click **Apply**. The Running Configuration file is updated. with the STP Global settings.

Defining Spanning Tree Interface Settings

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

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

To configure STP on an interface:

-
- STEP 1** Click **Spanning Tree > STP Interface Settings**. The *STP Interface Settings* page displays.
- STEP 2** Select an interface and click **Edit**. The *Edit Interface Settings* page displays.
- STEP 3** Enter the parameters
- **Interface**—Select the port number or LAG on which Spanning Tree is configured.
 - **STP**—Enables or disables STP on the port.
 - **Edge Port**—Enables or disables Fast Link on the port. If Fast Link mode is enabled for a port, the port state is automatically placed in the Forwarding state when the port link is up. Fast Link optimizes the STP protocol convergence. The options are:
 - *Enable*—Enables Fast Link immediately.
 - *Auto*—Enables Fast Link a few seconds after the interface becomes active. This allows STP to resolve loops before enabling Fast Link.
 - *Disable*—Disables Fast Link.
 - **BPDU Handling**—Select how BPDU packets are managed when STP is disabled on the port or the switch. BPDUs are used to transmit spanning tree information.
 - *Use Global Settings*—Select to use the settings defined in the *STP Status and Global Settings* page.
 - *Filtering*—Filters BPDU packets when Spanning Tree is disabled on an interface.
 - *Flooding*—Floods BPDU packets when Spanning Tree is disabled on an interface.

- **Path Cost**—Set the port contribution to the root path cost or use the default cost generated by the system.
 - **Priority**—Set the priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority is a value from 0 to 240, set in increments of 16.
 - **Port State**—Displays the current STP state of a port.
 - *Disabled*—STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
 - *Blocking*—The port is currently blocked, and cannot forward traffic (with the exception of BPDU data) or learn MAC addresses.
 - *Listening*—The port is in Listening mode. The port cannot forward traffic, and cannot learn MAC addresses.
 - *Learning*—The port is in Learning mode. The port cannot forward traffic, but it can learn new MAC addresses.
 - *Forwarding*—The port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
 - **Designated Bridge ID**—Displays the bridge priority and the MAC address of the designated bridge.
 - **Designated Port ID**—Displays the priority and interface of the selected port.
 - **Designated Cost**—Displays the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
 - **Forward Transitions**—Displays the number of times the port has changed from the **Blocking** state to **Forwarding** state.
 - **Speed**—Displays the speed of the port.
 - **LAG**—Displays the LAG to which the port belongs. If a port is a member of a LAG, the LAG settings override the port settings.
- STEP 4** Click **Apply**. The interface settings are modified, and the Running Configuration file is updated.

Configuring Rapid Spanning Tree Settings

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

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

To enter RSTP settings:

- STEP 1** Click **Spanning Tree > STP Status and Global Settings**. The *STP Status and Global Settings* page displays. Enable **RSTP**.
- STEP 2** Click **Spanning Tree > RSTP Interface Settings**. The *RSTP Interface Settings* page opens:
- STEP 3** Select a port. (Activate Protocol Migration is only available after selecting the port connected to the bridge partner being tested.)
- STEP 4** If a link partner is discovered by using STP, click **Activate Protocol Migration** to run a Protocol Migration test. This discovers whether the link partner using STP still exists, and if so whether it has migrated to RSTP. If it still exists as an STP link, the device continues to communicate with it by using STP. Otherwise, if it has been migrated to RSTP, the device communicates with it using RSTP.
- STEP 5** Select an interface, and click **Edit**. The *Edit Rapid Spanning Tree* page displays.
- STEP 6** Enter the parameters
 - **Interface**—Set the interface, and specify the port or LAG where RSTP is to be configured.
 - **Point to Point Administrative Status**—Define the point-to-point link status. Ports defined as Full Duplex are considered Point-to-Point port links.
 - *Enable*—This port is a RSTP edge port when this feature is enabled, and brings it to Forwarding mode quickly (usually within 2 seconds).
 - *Disable*—The port is not considered point-to-point for RSTP purposes, which means that STP works on it at regular speed, as opposed to rapid speed.
 - *Auto*—Automatically determines switch status by using RSTP BPDUs.
 - **Point to Point Operational Status**—Displays the Point-to-Point operating status if the **Point to Point Administrative Status** is set to Auto.

- **Role**—Displays the role of the port that has been assigned by STP to provide STP paths. The possible roles are:
 - *Root*—Lowest cost path to forward packets to the Root Bridge.
 - *Designated*—The interface through which the bridge is connected to the LAN, that provides the lowest cost path from the LAN to the Root Bridge.
 - *Alternate*—Provides an alternate path to the Root Bridge from the root interface.
 - *Backup*—Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
 - *Disabled*—The port is not participating in Spanning Tree.
- **Mode**—Displays the current Spanning Tree mode: Classic STP or RSTP.
- **Fast Link Operational Status**—Displays whether the Fast Link (Edge Port) is enabled, disabled, or automatic for the interface. The values are:
 - *Enabled*—Fast Link is enabled.
 - *Disabled*—Fast Link is disabled.
 - *Auto*—Fast Link mode is enabled a few seconds after the interface becomes active.
- **Port Status**—Displays the RSTP status on the specific port.
 - *Disabled*—STP is currently disabled on the port.
 - *Blocking*—The port is currently blocked, and it cannot forward traffic or learn MAC addresses.
 - *Listening*—The port is in Listening mode. The port cannot forward traffic, and cannot learn MAC addresses.
 - *Learning*—The port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
 - *Forwarding*—The port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.

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

MSTP Workflow

Managing MAC Address Tables

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

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

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

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

- [Configuring Static MAC Addresses](#)
- [Dynamic MAC Addresses](#)

Configuring Static MAC Addresses

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

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

To define a static address:

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

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

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

STEP 3 Enter the parameters.

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

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

Dynamic MAC Addresses

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

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

The dynamic addresses can be queried in the *Dynamic Addresses* page.

Setting Dynamic MAC Address Settings

Setting Dynamic MAC Address Settings

To enter the aging interval for dynamic addresses:

-
- STEP 1** Click **MAC Address Tables > Dynamic Address Settings**. The *Dynamic Addresses Setting* page opens.
 - STEP 2** Enter **Aging Time**. The aging time is a value between the user-configured value and twice that value minus 1. For example, if you entered 300 seconds, the aging time is between 300 and 599 seconds.
 - STEP 3** Click **Apply**. The Dynamic MAC Address Table is updated.
-

Querying Dynamic Addresses

Querying Dynamic Addresses

To view all dynamic addresses or a subset:

-
- STEP 1** Click **MAC Address Tables > Dynamic Addresses**. The *Dynamic Addresses* page opens.
 - STEP 2** In the *Filter* block, enter the following query criteria:
 - **VLAN ID**—Enter the VLAN ID for which the table is queried.
 - **MAC Address**—Enter the MAC address for which the table is queried.
 - **Interface**—Select the interface for which the table is queried. The query can search for specific ports or LAGs.
 - **Dynamic Address Table Sort Key**—Enter the field by which the table is sorted. The address table can be sorted by VLAN ID, MAC address, or interface.
 - STEP 3** Select the preferred option for sorting the addresses table in the Dynamic Address Sort Key. The table sort only affects the page under view. It does not sort the entire table.
 - STEP 4** Click **Go**. The Dynamic MAC Address Table is queried and the results are displayed.

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

Configuring Multicast Forwarding

This section describes the Multicast Forwarding feature, and contains the following topics:

- **Multicast Forwarding**
- **Defining Multicast Properties**
- **Adding MAC Group Address**
- **Adding IP Multicast Group Addresses**
- **Configuring IGMP Snooping**
- **MLD Snooping**
- **Querying IGMP/MLD IP Multicast Group**
- **Defining Multicast Router Ports**
- **Defining Forward All Multicast**
- **Defining Unregistered Multicast Settings**

Multicast Forwarding

Multicast forwarding enables one-to-many information dissemination. Multicast applications are useful for dissemination of information to multiple clients, where clients do not require reception of the entire content. A typical application is a cable-TV-like service, where clients can join a channel in the middle of a transmission, and leave before it ends.

The data is sent only to relevant ports. Forwarding the data only to the relevant ports conserves bandwidth and host resources on links.

For Multicast forwarding to work across IP subnets, nodes, and routers must be Multicast-capable. A Multicast-capable node must be able to:

- Send and receive Multicast packets.
- Register the Multicast addresses being listened to by the node with local routers, so that local and remote routers can route the Multicast packet to the nodes.

Typical Multicast Setup

While Multicast routers route Multicast packets between IP subnets, Multicast-capable Layer 2 switches forward Multicast packets to registered nodes within a LAN or VLAN.

A typical setup involves a router that forwards the Multicast streams between private and/or public IP networks, a switch with Internet Group Membership Protocol (IGMP) snooping capabilities, or Multicast Listener Discovery (MLD) snooping, and a Multicast client that wants to receive a Multicast stream. In this setup, the router sends IGMP queries periodically.

NOTE MLD for IPv6 is derived from the IGMP v2 for IPv4. Even though the description in this section is mostly for IGMP, it also describes coverage of MLD where implied.

These queries reach the switch, which in turn floods the queries to the VLAN, and also learns the port where there is a Multicast router (Mrouter). When a host receives the IGMP query message, it responds with an IGMP Join message saying that the host wants to receive a specific Multicast stream and optionally from a specific source. The switch with the IGMP snooping analyzes the Join messages, and learns that the Multicast stream the host has requested must be forwarded to this specific port. It then forwards the IGMP Join to the Mrouter only. Similarly, when the Mrouter receives an IGMP Join message, it learns the interface from which it received the Join messages that wants to receive a specific Multicast stream. The Mrouter forwards the requested Multicast stream to the interface.

Multicast Operation

Multicast Operation

In a Layer 2 Multicast service, a Layer 2 switch receives a single frame addressed to a specific Multicast address. It creates copies of the frame to be transmitted on each relevant port.

When the switch is IGMP/MLD-snooping-enabled and receives a frame for a Multicast stream, it forwards the Multicast frame to all the ports that have registered to receive the Multicast stream using IGMP Join messages.

The switch can forward Multicast streams based on one of the following options:

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

One of these options can be configured per VLAN.

The system maintains lists of Multicast groups for each VLAN, and this manages the Multicast information that each port should receive. The Multicast groups and their receiving ports can be configured statically or learned dynamically using IGMP or Multicast Listener Discovery (MLD) protocols snooping.

Multicast Registration

Multicast Registration

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

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

When a switch learns that a host is using IGMP/MLD messages to register to receive a Multicast stream, optionally from a specific source, the switch adds the registration to its Multicast Forwarding Data Base (MFDB).

IGMP/MLD snooping can effectively reduce Multicast traffic from streaming bandwidth-intensive IP applications. A switch using IGMP/MLD snooping only forwards Multicast traffic to the hosts interested in that traffic. This reduction of Multicast traffic reduces the packet processing at the switch, and also reduces the workload of the end hosts, since they do not have to receive and filter all of the Multicast traffic generated in the network.

The following versions are supported:

- IGMP v1/v2/ v3
- MLD v1/v2

Multicast Address Properties

Multicast addresses have the following properties:

- Each IPv4 Multicast address is in the address range 224.0.0.0 to 239.255.255.255.
- The IPv6 Multicast address is FF00:/8.
- To map an IP Multicast group address to an Layer 2 Multicast address:
 - For IPv4, this is mapped by taking the 23 low-order bits from the IPv4 address, and adding them to the 01:00:5e prefix. By standard, the upper nine bits of the IP address are ignored, and any IP addresses that only differ in the value of these upper bits are mapped to the same Layer 2 address, since the lower 23 bits that are used are identical. For example, 234.129.2.3 is mapped to a MAC Multicast group address 01:00:5e:01:02:03. Up to 32 IP Multicast group addresses can be mapped to the same Layer 2 address.
 - For IPv6, this is mapped by taking the 32 low-order bits of the Multicast address, and adding the prefix of 33:33. For example, the IPv6 Multicast address FF00:1122:3344 is mapped to Layer 2 Multicast 33:33:11:22:33:44.

Defining Multicast Properties

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

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

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

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

The following are ways of forwarding Multicast frames:

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

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

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

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

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

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

To enable Multicast filtering, and select the forwarding method:

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

STEP 2 Enter the parameters.

- **Bridge Multicast Filtering Status**—Select to enable filtering.
- **VLAN ID**—Select the VLAN ID to set its forwarding method.
- **Forwarding Method for IPv6**—Set one of the following forwarding methods for IPv6 addresses: MAC Group Address, IP Group Address, or Source Specific IP Group Address.
- **Forwarding Method for IPv4**—Set one of the following forwarding methods for IPv4 addresses: MAC Group Address, IP Group Address, or Source Specific IP Group Address.

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

Adding MAC Group Address

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

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

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

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

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

To define and view MAC Multicast groups:

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

STEP 2 Enter the parameters.

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

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

Entries that were created both in this page and in the *IP Multicast Group Address* page are displayed. For those created in the *IP Multicast Group Address page*, the IP addresses are converted to MAC addresses.

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

STEP 5 Enter the parameters.

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

STEP 6 Click **Apply**, the MAC Multicast group is added, and the Running Configuration file is updated.

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

The page displays:

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

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

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

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

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

STEP 10 Click **Apply**, and the Running Configuration file is updated.

NOTE Entries that were created in the *IP Multicast Group Address* page cannot be deleted in this page (even if they are selected).

Adding IP Multicast Group Addresses

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

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

To define and view IP Multicast groups:

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

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

STEP 2 Enter the parameters required for filtering.

- **VLAN ID equals to**—Define the VLAN ID of the group to be displayed.
- **IP Version equals to**—Select IPv6 or IPv4.
- **IP Multicast Group Address equals to**—Define the IP address of the Multicast group to be displayed. This is only relevant when the Forwarding mode is (S,G).

- **Source IP Address equals to**—Define the source IP address of the sending device. If mode is (S,G), enter the sender S. This together with the IP Group Address is the Multicast group ID (S,G) to be displayed. If mode is (*.G), enter an * to indicate that the Multicast group is only defined by destination.
- STEP 3** Click **Go**. The results are displayed in the lower block. When Bonjour and IGMP are enabled on switch in Layer 2 mode, the IP Multicast address of Bonjour is displayed.
- STEP 4** Click **Add** to add a static IP Multicast Group Address. The *Add IP Multicast Group Address* page opens.
- STEP 5** Enter the parameters.
- **VLAN ID**—Defines the VLAN ID of the group to be added.
 - **IP Version**—Select the IP address type.
 - **IP Multicast Group Address**—Define the IP address of the new Multicast group.
 - **Source Specific**—Indicates that the entry contains a specific source, and adds the address in the IP Source Address field. If not, the entry is added as a (*.G) entry, an IP group address from any IP source.
 - **IP Source Address**—Defines the source address to be included.
- STEP 6** Click **Apply**. The IP Multicast group is added, and the device is updated.
- STEP 7** To configure and display the registration of an IP group address, select an address and click **Details**. The *IP Multicast Interface Settings* page opens.

The VLAN ID, IP Version, IP Multicast Group Address, and Source IP Address selected are displayed as read-only in the top of the window. You can select the filter type:

- **Interface Type equals to**—Select whether to display ports or LAGs.
- STEP 8** For each interface, select its association type. The options are as follows:
- **Static**—Attaches the interface to the Multicast group as a static member.
 - **Forbidden**—Specifies that this port is forbidden from joining this group on this VLAN.
 - **None**—Indicates that the port is not currently a member of this Multicast group on this VLAN. This is selected by default until Static or Forbidden is selected.

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

Configuring IGMP Snooping

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

Additional Information

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

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

When IGMP Snooping is enabled globally or on a VLAN, all IGMP packets are forwarded to the CPU. The CPU analyzes the incoming packets, and determines the following:

- Which ports are asking to join which Multicast groups on what VLAN.
- Which ports are connected to Multicast routers (Mrouters) that are generating IGMP queries.
- Which ports are receiving PIM, DVMRP, or IGMP query protocols.

These are displayed on the *IGMP Snooping* page.

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

To enable IGMP Snooping and identify the switch as an IGMP Snooping Querier on a VLAN:

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

STEP 2 Enable or disable the IGMP Snooping status.

When IGMP Snooping is enabled globally, the device monitoring network traffic can determine which hosts have requested to receive Multicast traffic.

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

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

STEP 4 Enter the parameters.

- **VLAN ID**—Select the VLAN ID on which IGMP snooping is defined.
- **IGMP Snooping Status**—Enable or disable the monitoring of network traffic for the selected VLAN.
- **Operational IGMP Snooping Status**—Displays the current status of the IGMP Snooping for the selected VLAN.
- **MRouter Ports Auto Learn**—Enable or disable auto learning of the ports to which the Mrouter is connected.
- **Query Robustness**—Enter the Robustness Variable value to be used if this switch is the elected querier.
- **Operational Query Robustness**—Displays the robustness variable sent by the elected querier.
- **Query Interval**—Enter the interval between the General Queries to be used if this switch is the elected querier.
- **Operational Query Interval**—The time interval in seconds between General Queries sent by the elected querier.
- **Query Max Response Interval**—Enter the delay used to calculate the Maximum Response Code inserted into the periodic General Queries.
- **Operational Query Max Response Interval**—Displays the Query Max Response Interval included in the General Queries sent by the elected querier.

- **Last Member Query Counter**—Enter the number of IGMP Group-Specific Queries sent before the switch assumes there are no more members for the group, if the switch is the elected querier.
- **Operational Last Member Query Counter**—Displays the operational value of the Last Member Query Counter.
- **Last Member Query Interval**—Enter the Maximum Response Delay to be used if the switch cannot read Max Response Time value from group-specific queries sent by the elected querier.
- **Operational Last Member Query Interval**—Displays the Last Member Query Interval sent by the elected querier.
- **Immediate Leave**—Enable Immediate Leave to decrease the time it takes to block a Multicast stream sent to a member port when an IGMP Group Leave message is received on that port.

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

MLD Snooping

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

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

IGMP/MLD snooping can effectively reduce Multicast traffic from streaming bandwidth-intensive IP applications. A switch using IGMP/MLD snooping only forwards Multicast traffic to the hosts interested in that traffic. This reduction of Multicast traffic reduces the packet processing at the switch, and also reduces the workload at the end hosts, since they do not have to receive and filter all of the Multicast traffic generated in the network.

The following versions are supported:

- IGMP v1/v2/ v3
- MLD v1/v2

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

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

The switch uses this feature to build Multicast membership lists. It uses the lists to forward Multicast packets only to switch ports where there are host nodes that are members of the Multicast groups. The switch does not support MLD Querier.

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

Additional Information

The switch supports two versions of MLD snooping:

- MLDv1 snooping detects MLDv1 control packets, and sets up traffic bridging, based on IPv6 destination Multicast addresses.
- MLDv2 snooping uses MLDv2 control packets to forward traffic based on the source IPv6 address, and the destination IPv6 Multicast address.

The actual MLD version is selected by the Multicast router in the network.

In an approach similar to IGMP snooping, MLD frames are snooped as they are forwarded by the switch from stations to an upstream Multicast router and vice versa. This facility enables a switch to conclude the following:

- On which ports stations interested in joining a specific Multicast group are located
- On which ports Multicast routers sending Multicast frames are located

This knowledge is used to exclude irrelevant ports (ports on which no stations have registered to receive a specific Multicast group) from the forwarding set of an incoming Multicast frame.

If you enable MLD snooping in addition to the manually-configured Multicast groups, the result is a union of the Multicast groups and port memberships derived from the manual setup and the dynamic discovery by MLD snooping. Only static definitions are preserved when the system is rebooted.

To enable MLD Snooping:

-
- STEP 1** Click **Multicast > MLD Snooping**. The *MLD Snooping* page opens.
- STEP 2** Enable or disable **MLD Snooping Status**. When MLD Snooping is globally enabled, the device monitoring network traffic can determine which hosts have requested to receive Multicast traffic. The switch performs MLD Snooping only if both MLD snooping and Bridge Multicast filtering are enabled.
- STEP 3** Select a VLAN, and click **Edit**. The *Edit MLD Snooping* page opens.
- STEP 4** Enter the parameters.
- **VLAN ID**—Select the VLAN ID.
 - **MLD Snooping Status**—Enable or disable MLD snooping on the VLAN. The switch monitors network traffic to determine which hosts have asked to be sent Multicast traffic. The switch performs MLD snooping only when MLD snooping and Bridge Multicast filtering are both enabled
 - **Operational MLD Snooping Status**—Displays the current status of MLD Snooping for the selected VLAN.
 - **MRouter Ports Auto-Learn**—Enable or disable Auto Learn for the Multicast router.
 - **Query Robustness**—Enter the Robustness Variable value to be used if the switch cannot read this value from messages sent by the elected querier.
 - **Operational Query Robustness**—Displays the robustness variable sent by the elected querier.
 - **Query Interval**—Enter the Query Interval value to be used by the switch if the switch cannot derive the value from the messages sent by the elected querier.
 - **Operational Query Interval**—The time interval in seconds between General Queries received from the elected querier.
 - **Query Max Response Interval**—Enter Query Max Response delay to be used if the switch cannot read the Max Response Time value from General Queries sent by the elected querier.
 - **Operational Query Max Response Interval**—Displays the delay used to calculate the Maximum Response Code inserted into the General Queries.

- **Last Member Query Counter**—Enter the Last Member Query Count to be used if the switch cannot derive the value from the messages sent by the elected querier.
- **Operational Last Member Query Counter**—Displays the operational value of the Last Member Query Counter.
- **Last Member Query Interval**—Enter the Maximum Response Delay to be used if the switch cannot read Max Response Time value from Group-Specific queries sent by the elected querier.
- **Operational Last Member Query Interval**—The Last Member Query Interval sent by the elected querier.
- **Immediate Leave**—When enabled, reduces the time it takes to block unnecessary MLD traffic sent to a switch port.

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

Querying IGMP/MLD IP Multicast Group

The *IGMP/MLD IP Multicast Group* page displays the IPv4 and IPv6 group address learned from IGMP/MLD messages.

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

To query for a IP Multicast group:

- STEP 1** Click **Multicast > IGMP/MLD IP Multicast Group**. The *IGMP/MLD IP Multicast Group* page opens.
- STEP 2** Set the type of snooping group for which to search: IGMP or MLD.
- STEP 3** Enter some or all of following query filter criteria:
 - **Group Address equals to**—Defines the Multicast group MAC address or IP address to query.

- **Source Address equals to**—Defines the sender address to query.
- **VLAN ID equals to**—Defines the VLAN ID to query.

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

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

Defining Multicast Router Ports

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

To statically configure or see dynamically-detected ports connected to the Multicast router:

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

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

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

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

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

- **Static**—The port is statically configured as a Multicast router port.
- **Dynamic**—(Display only) The port is dynamically configured as a Multicast router port by a MLD/IGMP query. To enable the dynamic learning of Multicast router ports, go to the **Multicast > IGMP Snooping** page, and the **Multicast > MLD Snooping** page
- **Forbidden**—This port is not to be configured as a Multicast router port, even if IGMP or MLD queries are received on this port. If **Auto Detect Mrouter Ports** is enabled on this port, the configuration does not succeed.
- **None**—The port is not currently a Multicast router port.

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

Defining Forward All Multicast

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

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

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

NOTE The configuration affects only the ports that are members of the selected VLAN.

To define Forward All Multicast:

STEP 1 Click **Multicast > Forward All**. The *Forward All* page opens.

STEP 2 Define the following:

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

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

-
- STEP 4** Select the port/LAG that is to be defined as Forward All by using the following methods:
- **Static**—The port receives all Multicast streams.
 - **Forbidden**—Ports cannot receive any Multicast streams, even if IGMP/MLD snooping designated the port to join a Multicast group.
 - **None**—The port is not currently a Forward All port.
- STEP 5** Click **Apply**. The Running Configuration file is updated.
-

Defining Unregistered Multicast Settings

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

The switch forwards Multicast frames (from a registered Multicast group) only to ports that are registered to that Multicast group.

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

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

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

To define unregistered Multicast settings:

-
- STEP 1** Click **Multicast > Unregistered Multicast**. The *Unregistered Multicast* page opens.
- STEP 2** Define the following:
- **Interface Type equals to**—The view as all ports or all LAGs.
 - **Port/LAG**—Displays the port or LAG ID.

- **Unregistered Multicast**—Displays the forwarding status of the selected interface. The possible values are:
 - *Forwarding*—Enables forwarding of unregistered Multicast frames to the selected interface.
 - *Filtering*—Enables filtering (rejecting) of unregistered Multicast frames to the selected interface.

STEP 3 Click **Apply**. The settings are saved, and the Running Configuration file is updated.

Configuring IP Information

IP interface addresses can be configured manually by the user, or automatically configured by a DHCP server. This section provides information for defining the switch IP addresses.

It includes the following topics:

- [Management and IP Interfaces](#)
- [Configuring ARP](#)
- [Domain Name Systems](#)

Management and IP Interfaces

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

Layer 2 IP Addressing

Layer 2 IP Addressing

The switch has a single IP address in the management VLAN. This IP address and the default gateway can be configured manually, or by DHCP. The static IP address and default gateway are configured on the *IPv4 Interface* page. The switch uses the default gateway, if configured, to communicate with devices that are not in the same IP subnet as the switch. By default, VLAN 1 is the management VLAN, but this can be modified. The switch can only be reached at the configured IP address through its management VLAN.

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

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

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

IP address collisions occur when the same IP address is used in the same IP subnet by more than one device. Address collisions require administrative actions on the DHCP server and/or the devices that collide with the switch.

When a VLAN is configured to use dynamic IP addresses, the switch issues DHCP requests until it is assigned an IP address from a DHCP server. The management VLAN can be configured with a static or dynamic IP address. The IP subnets to which these IP addresses belong are known as directly connected/attached IP subnets.

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

- Unless the switch is configured with a static IP address, it issues DHCP queries until a response is received from a DHCP server.
- If the IP address on the switch is changed, the switch issues gratuitous ARP packets to the corresponding VLAN to check IP address collisions. This rule also applies when the switch reverts to the default IP address.
- The system status LED changes to solid green when a new unique IP address is received from the DHCP server. If a static IP address has been set, the system status LED also changes to solid green. The LED flashes when the switch is acquiring an IP address and is currently using the factory default IP address 192.168.1.254.
- The same rules apply when a client must renew the lease, prior to its expiration date through a DHCPREQUEST message.
- When no statically defined or DHCP-acquired IP address is available, the default IP address is used. When the other IP addresses becomes available, the addresses are automatically used. The default IP address is always on the management VLAN.

Defining an IPv4 Interface

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

To configure the IPv4 switch IP address:

STEP 1 Click **Administration > Management Interface > (Layer 2) > IPv4 Interface**. The *IPv4 Interface* page opens.

STEP 2 Enter values for the following fields:

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

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

- **IP Address**—Enter the IP address, and configure one of the following fields:
- **Mask**—Select and enter the IP address mask.
- **Prefix Length**—Select and enter the length of the IPv4 address prefix.
- **Administrative Default Gateway**—Select User Defined and enter the default gateway IP address, or select None to remove the selected default gateway IP address from the interface.
- **Operational Default Gateway**—Displays the current default gateway status.

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

If a dynamic IP address is retrieved from the DHCP server, select those of the following fields that are enabled:

- **Renew IP Address Now**—The switch dynamic IP address can be renewed any time after it is assigned by a DHCP server. Depending on your DHCP server configuration, the switch might receive a new IP address after the renewal that will cause a loss of connectivity to the web-based switch configuration utility.
- **Auto Configuration via DHCP**—Displays status of auto-configuration feature. You can configure DHCP Auto Configuration from *Administration > File Management > DHCP Auto Configuration*.

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

Managing IPv6

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

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

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

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

The switch detects IPv6 frames by the IPv6 Ethertype.

Defining IPv6 Global Configuration

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

To define IPv6 global parameters:

STEP 1 Click **Administration > Management Interface (Layer 2) > IPv6 Global Configuration**.

The *IPv6 Global Configuration* page opens.

STEP 2 Enter values for the following fields:

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

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

Defining an IPv6 Interface

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

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

To configure IPv6 interfaces:

STEP 1 Click **Administration > Management Interface (Layer 2) > IPv6 Interfaces**.

The *IPv6 Interface* page opens.

This page displays the IPv6 interfaces already configured.

STEP 2 Click **Add** to add a new interface on which interface IPv6 is enabled.

STEP 3 The *Add IPv6 Interface* page opens.

STEP 4 Enter the values.

- **IPv6 Interface**—Select a specific port, LAG, VLAN, or ISATAP tunnel.
 - **Number of DAD Attempts**—Enter the number of consecutive neighbor solicitation messages that are sent while Duplicate Address Detection (DAD) is performed on the interface's Unicast IPv6 addresses. DAD verifies the uniqueness of a new Unicast IPv6 address before it is assigned. New addresses remain in a tentative state during DAD verification. Entering **0** in this field disables duplicate address detection processing on the specified interface. Entering **1** in this field indicates a single transmission without follow-up transmissions.
 - **IPv6 Address Auto Configuration**—Enable automatic address configuration from the DHCP server. If enabled, the switch supports IPv6 stateless address auto configuration of site local and global IP address from the IPv6 router advertisement received on the interface. The switch does not support stateful address auto configuration.
 - **Send ICMPv6 Messages**—Enable generating unreachable destination messages.
- STEP 5** Click **Apply** to enable IPv6 processing on the selected interface. Regular IPv6 interfaces have the following addresses automatically configured:
- Link local address using EUI-64 format interface ID based on a device's MAC address
 - All node link local Multicast addresses (FF02::1)
 - Solicited-Node Multicast address (format FF02::1:FFXX:XXXX)
- STEP 6** Click **IPv6 Address Table** to manually assign IPv6 addresses to the interface, if required. This page is described in the [Defining IPv6 Addresses](#) section.

Defining IPv6 Addresses

To assign an IPv6 address to an IPv6 Interface:

- STEP 1** Click **Administration > Management Interface (Layer 2) > IPv6 Addresses**
- The *IPv6 Addresses* page opens.
- STEP 2** Select an interface name, and click **Go**. The interface is displayed in the IPv6 Address Table.

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

STEP 4 Enter values for the fields.

- **IPv6 Interface**—Displays the interface where the address is automatically completed, based on the filter.
- **IPv6 Address Type**—Select Link Local or Global as the type of IPv6 address to add.
 - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
 - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- **IPv6 Address**—The switch supports one IPv6 interface. In addition to the default link local and Multicast addresses, the device also automatically adds global addresses to the interface based on the router advertisements it receives. The device supports a maximum of 128 addresses at the interface. Each address must be a valid IPv6 address that is specified in hexadecimal format by using 16-bit values separated by colons.

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

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

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

Defining an IPv6 Default Router List

The *IPv6 Default Router List* page enables configuring and viewing the default IPv6 router addresses. This list contains the routers that are candidates to become the switch default router for non-local traffic (it may be empty). The switch randomly selects a router from the list. The switch supports one static IPv6 default router. Dynamic default routers are routers that have sent router advertisements to the switch IPv6 interface.

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

- When removing an IP interface, all the default router IP addresses are removed.
- Dynamic IP addresses cannot be removed.
- An alert message is displayed after an attempt is made to insert more than a single user-defined address.
- An alert message is displayed when attempting to insert a non-link local type address, meaning 'fe80:'.

To define a default router:

-
- STEP 1** Click **Administration > Management Interface (Layer 2) > IPv6 Default Router List**.

The *IPv6 Default Router List* page opens.

This page displays the following fields for each default router:

- **Default Router IPv6 Address**—Link local IP address of the default router.
- **Interface**—Outgoing IPv6 interface where the default router resides.
- **Type**—The default router configuration that includes the following options:
 - *Static*—The default router was manually added to this table through the **Add** button.
 - *Dynamic*—The default router was dynamically configured.
- **State**—The default router status options are:
 - *Incomplete*—Address resolution is in process. Default router has not yet responded.
 - *Reachable*—Positive confirmation was received within the *Reachable Time*.

- *Stale*—Previously-known neighboring network is unreachable, and no action is taken to verify its reachability until it is necessary to send traffic.
- *Delay*—Previously-known neighboring network is unreachable. The device is in Delay state for a predefined *Delay Time*. If no confirmation is received, the state changes to Probe.
- *Probe*—Neighboring network is unavailable, and Unicast Neighbor Solicitation probes are being sent to verify the status.

STEP 2 Click **Add** to add a static default router. The *Add Default Router* page opens.

The window displays the Link Local Interface. The interface can be a port, LAG, VLAN, or tunnel.

STEP 3 Enter the static default router IP address in the Default Router IPv6 Address field.

STEP 4 Click **Apply**. The default router is defined, and the Running Configuration file is updated.

Configuring IPv6 Tunnels

The ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) enables encapsulating IPv6 packets within IPv4 packets for transmission over IPv4 networks. To configure a tunnel, do the following:

- Manually enable and configure an ISATAP tunnel.
- Manually define an IPv6 interface for the ISATAP tunnel.

After these actions, the switch automatically configures the link local IPv6 address to the IPv6 interface.

When defining ISATAP tunnels, note the following:

- An IPv6 link local address is assigned to the ISATAP interface. The initial IP address is assigned to the interface, which is then activated.
- If an ISATAP interface is active, the ISATAP router IPv4 address is resolved via DNS by using ISATAP-to-IPv4 mapping. If the ISATAP DNS record is not resolved, ISATAP host name-to-address mapping is searched in the host mapping table.
- When the ISATAP router IPv4 address is not resolved via the DNS process, the ISATAP IP interface remains active. The system does not have a default router for ISATAP traffic until the DNS process is resolved.

To configure an IPv6 Tunnel:

STEP 1 Click **Administration > Management Interface > (Layer 2) > IPv6 Tunnel**.

The *IPv6 Tunnel* page opens.

STEP 2 Enter values for the following fields:

- **Tunnel Number**—Displays the automatic tunnel router domain number.
- **Tunnel Type**—Always displayed as ISATAP.
- **Source IPv4 Address**—Disable the ISATAP tunnel, or enable the ISATAP tunnel over an IPv4 interface. The IPv4 address of the selected IPv4 interface used to form part of the IPv6 address over the ISATAP tunnel interface. The IPv6 address has a 64-bit network prefix of fe80::, with the rest of the 64-bit formed by concatenating 0000:5EFE and the IPv4 address.
 - *Auto*—Automatically selects the lowest IPv4 address from among all of its configured IPv4 interfaces.
 - *None*—Disable the ISATAP tunnel.
 - *Manual*—Manually configure an IPv4 address. The IPv4 address configured must be one of the IPv4 addresses at the switch IPv4 interfaces.
- **Tunnel Router's Domain Name**—A global string that represents a specific automatic tunnel router domain name. The name can either be the default name (ISATAP) or a user defined name.
- **Query Interval**—The number of seconds from 10-3600 between DNS queries (before the IP address of the ISATAP router is known) for this tunnel. The interval can be the default value (10 seconds) or a user defined interval.
- **ISATAP Solicitation Interval**—The number of seconds from 10-3600 between ISATAP router solicitations messages, when there is no active ISATAP router. The interval can be the default value (10 seconds) or a user defined interval.
- **ISATAP Robustness**—Used to calculate the interval for the DNS or router solicitation queries. The bigger the number, the more frequent the queries. The default value is 3. The range is 1-20.

NOTE The ISATAP tunnel is not operational if the underlying IPv4 interface is not in operation.

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

Defining IPv6 Neighbors Information

The *IPv6 Neighbors* page enables configuring and viewing the list of IPv6 neighbors on the IPv6 interface. The IPv6 Neighbor Table (also known as IPv6 Neighbor Discovery Cache) displays the MAC addresses of the IPv6 neighbors that are in the same IPv6 subnet as the switch. This is used to verify the reachability of this neighbor. This is the IPv6 equivalent of the IPv4 ARP Table. When the switch needs to communicate with its neighbors, the switch uses the IPv6 Neighbor Table to determine the MAC addresses based on their the IPv6 addresses.

This page displays the neighbors that were automatically detected or manually configured entries. Each entry displays to which interface the neighbor is connected, the neighbor's IPv6 and MAC addresses, the entry type (static or dynamic), and the state of the neighbor.

To define IPv6 neighbors:

STEP 1 Click **Administration > Management Interface > (Layer 2) > IPv6 Neighbors**

The *IPv6 Neighbors* page opens.

STEP 2 Select a **Clear Table** option to clear some or all of IPv6 addresses in the IPv6 Neighbors Table.

- **Static Only**—Deletes the static IPv6 address entries.
- **Dynamic Only**—Deletes the dynamic IPv6 address entries.
- **All Dynamic & Static**—Deletes the static and dynamic address entries IPv6 address entries.

The following fields are displayed for the neighboring interfaces:

- **Interface**—Neighboring IPv6 interface type.
- **IPv6 Address**—IPv6 address of a neighbor.
- **MAC Address**—MAC address mapped to the specified IPv6 address.
- **Type**—Neighbor discovery cache information entry type (static or dynamic).
- **State**—Specifies the IPv6 neighbor status. The values are:

- *Incomplete*—Address resolution is working. The neighbor has not yet responded.
- *Reachable*—Neighbor is known to be reachable.
- *Stale*—Previously-known neighbor is unreachable. No action is taken to verify its reachability until traffic must be sent.
- *Delay*—Previously-known neighbor is unreachable. The interface is in Delay state for a predefined Delay Time. If no reachability confirmation is received, the state changes to Probe.
- *Probe*—Neighbor is no longer known to be reachable, and Unicast Neighbor Solicitation probes are being sent to verify the reachability.

STEP 3 To add a neighbor to be monitored, click **Add**. The *Add IPv6 Neighbors* page opens.

STEP 4 Enter values for the following fields:

- **Interface**—The neighboring IPv6 interface to be added.
- **IPv6 Address**—Enter the IPv6 network address assigned to the interface. The address must be a valid IPv6 address.
- **MAC Address**—Enter the MAC address mapped to the specified IPv6 address.

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

STEP 6 To change the type of an IP address from Dynamic to Static, use the *Edit IPv6 Neighbors* page.

Viewing IPv6 Route Tables

The *IPv6 Routes* page displays the *IPv6 Routing Table*. The table contains a single default route (IPv6 address:0) that uses the default router selected from the IPv6 Default Router List to send packets to destination devices that are not in the same IPv6 subnet as the switch. In addition to the default route, the table also contains dynamic routes that are ICMP redirect routes received from IPv6 routers by using ICMP redirect messages. This could happen when the default router the switch uses is not the router for traffic to which the IPv6 subnets that the switch wants to communicate.

To view IPv6 routing entries:

STEP 1 Click **Administration > Management Interface > (Layer 2) > IPv6 Routes**.

The *IPv6 Routes* page opens.

This page displays the following fields:

- **IPv6 Address**—The IPv6 subnet address.
- **Prefix Length**—IP route prefix length for the destination IPv6 subnet address. It is preceded by a forward slash.
- **Interface**—Interface used to forward the packet.
- **Next Hop**—Address where the packet is forwarded. Typically, this is the address of a neighboring router. This must be a link local address.
- **Metric**—Value used for comparing this route to other routes with the same destination in the IPv6 router table. All default routes have the same value.
- **Life Time**—Time period during which the packet can be sent, and resent, before being deleted.
- **Route Type**—How the destination is attached, and the method used to obtain the entry. The following values are:
 - *Local*—A manually configured switch IPv6 address.
 - *Dynamic*—The destination is indirectly attached IPv6 subnet address. The entry was obtained dynamically via the ICMP protocol.

STEP 2 Click **Apply**. The IPv6 route is added, and Running Configuration file is updated.

DHCP Relay Description

DHCP Relay Limitations

Defining DHCP Relay Properties

Defining DHCP Relay Interfaces

Configuring ARP

The switch maintains an ARP (Address Resolution Protocol) table for all known devices that reside in its directly-connected IP subnets. A directly-connected IP subnet is the subnet to which a IPv4 interface of the switch is connected. When the switch needs to send/route a packet to a local device, it searches the ARP table to obtain the MAC address of the device. The ARP table contains both static and dynamic addresses. Static addresses are manually configured and do not age out. The switch creates dynamic addresses from the ARP packets it receives. Dynamic addresses age out after a configured time.

NOTE The IP/MAC address mapping information in the ARP Table is used by the switch to forward traffic originated by the switch.

To define the ARP tables:

STEP 1 Click **IP Configuration > ARP (Layer 2)**. The *ARP Table* page opens.

STEP 2 Enter the parameters.

- **ARP Entry Age Out**—Enter the number of seconds that dynamic addresses can remain in the ARP table. A dynamic address ages out after the time it is in the table exceeds the ARP Entry Age Out time. When a dynamic address ages out, it is deleted from the table, and only returns when it is relearned.
- **Clear ARP Table Entries**—Select the type of ARP entries to be cleared from the system.
 - *All*—Deletes all of the static and dynamic addresses immediately.
 - *Dynamic*—Deletes all of the dynamic addresses immediately.
 - *Static*—Deletes all of the static addresses immediately.

- *Normal Age Out*—Deletes dynamic addresses based on the configured ARP Entry Age Out time.

STEP 3 Click **Apply**. The ARP global settings are modified, and the Running Configuration file is updated.

The ARP table displays the following fields:

- **Interface**—The IPv4 Interface of the directly-connected IP subnet where the IP device resides.
- **IP Address**—The IP address of the IP device.
- **MAC Address**—The MAC address of the IP device.
- **Status**—Whether the entry was manually entered or dynamically learned.

STEP 4 Click **Add**. The *Add ARP Entry* page opens.

STEP 5 Enter the parameters:

- **IP Version**—The IP address format supported by the host. Only IPv4 is supported.
- **Interface**—IPv4 interface on the switch.

There is only one directly-connected IP subnet, which is always in the management VLAN. All the static and dynamic addresses in the ARP Table reside in the management VLAN.

- **IP Address**—Enter the IP address of the local device.
- **MAC Address**—Enter the MAC address of the local device.

STEP 6 Click **Apply**. The ARP entry is defined, and the Running Configuration file is updated.

Domain Name Systems

The Domain Name System (DNS) translates user-defined domain names into IP addresses for the purpose of locating and addressing these objects.

As a DNS client the switch resolves domain names to IP addresses through one or more configured DNS servers.

Defining DNS Servers

Use the *DNS Servers* page to enable the DNS feature, configure the DNS servers and set the default domain used by the switch.

STEP 1 Click **IP Configuration > Domain Name System > DNS Servers**. The *DNS Servers* page opens.

STEP 2 Enter the parameters.

- **DNS**—Select to designate the switch as a DNS client which resolves DNS names into IP addresses through one or more configured DNS servers.
- **Default Domain Name**—Enter the default DNS domain name (1–158 characters). The switch appends this to all non-fully qualified domain names (FQDNs) turning them into FQDNs.
- **Type**—Displays the default domain type options:
 - *DHCP*—The default domain name is dynamically assigned by the DHCP server.
 - *Static*—The default domain name is user-defined.
 - *N/A*—No default domain name.

DNS Server Table:

- **DNS Server**—The IP addresses of the DNS servers. Up to eight DNS servers can be defined.
- **Server State**—The active DNS server. There can be only one active server. Each static server has a priority, a lower value means a higher priority. When first time the request is sent, static server with lowest priority is chosen. If after two retries there is no response from this server, the next server with the next lowest priority is selected. If none of the static servers respond, the first dynamic server on the table, sorted by IP address (low to high), is selected.

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

STEP 4 To add a DNS server, click **Add**. The *Add DNS Server* page opens.

STEP 5 Enter the parameters.

- **IP Version**—Select Version 6 for IPv6 or Version 4 for IPv4.

- **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are:
 - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
 - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- **Link Local Interface**—If the IPv6 address type is Link Local, select whether it is received through VLAN2 or ISATAP.
- **DNS Server IP Address**—Enter the DNS server IP address.
- **Set DNS Server Active**—Select to activate the new DNS server.

STEP 6 Click **Apply**. The DNS server is added, and the Running Configuration file is updated.

Mapping DNS Hosts

The switch saves frequently-queried domain names acquired from the DNS servers in a local DNS cache. The cache can hold up to 64 static entries, 64 dynamic entries, and one entry for each IP address configured on the switch by DHCP. Name resolution always begins by checking static entries, continues by checking the dynamic entries, and ends by sending requests to the external DNS server.

Several IP addresses are supported per DNS per host name.

To add a domain name and its IP address:

STEP 1 Click **IP Configuration > Domain Name System > Host Mapping**. The *Host Mapping* page opens.

This page displays the following fields:

- **Host Name**—User-defined domain name, up to 158 characters.
- **IP Address**—The host name IP address.

STEP 2 To add a host mapping, click **Add**. The *Add Host Mapping* page opens.

STEP 3 Enter the parameters.

- **IP Version**—Select Version 6 for IPv6 or Version 4 for IPv4.
- **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are:
 - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
 - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- **Link Local Interface**—If the IPv6 address type is Link Local, select whether it is received through VLAN2 or ISATAP.
- **Host Name**—Enter a domain name, up to 158 characters.
- **IP Address**—Enter an IPv4 address or enter up to four IPv6 host addresses. Addresses 2–4 are backup addresses.

STEP 4 Click **Apply**. The DNS host is added, and the Running Configuration file is updated.

Configuring Security

This section describes switch security and access control. The system handles various types of security.

The following list of topics describes the various types of security features described in this section. Some features are used for more than a single type of security or control, and so they appear twice in the list of topics below.

Permission to administer the switch is described in the following sections:

- **Setting Password Complexity Rules**
- **Configuring RADIUS Parameters**
- **Configuring Management Access Authentication**
- **Defining Access Profiles**
- **Configuring TCP/UDP Services**

Protection from attacks directed at the switch CPU is described in the following sections:

- **Configuring TCP/UDP Services**
- **Defining Storm Control**

Access control of end-users to the network through the switch is described in the following sections:

- **Configuring Management Access Authentication**
- **Defining Access Profiles**
- **Setting Password Complexity Rules**
- **Configuring RADIUS Parameters**
- **Configuring Port Security**
- **Configuring 802.1X**

Protection from other network users is described in the following sections. These are attacks that pass through, but are not directed at, the switch.

- [Denial of Service Prevention](#)
- [Configuring TCP/UDP Services](#)
- [Defining Storm Control](#)
- [Configuring Port Security](#)

Defining Users

The default username/password is **cisco/cisco**. The first time that you log in with the default username and password, you are required to enter a new password. Password complexity is enabled by default. If the password that you choose is not complex enough (**Password Complexity Settings** are enabled in the *Password Strength* page), you will be prompted to create another password.

Setting User Accounts

Setting User Accounts

The *User Accounts* page enables entering additional users that are permitted to access to the switch (read-only or read-write) or changing the passwords of existing users.

NOTE It is not permitted to delete all users. If all users are selected, the **Delete** button is disabled.

To add a new user:

STEP 1 Click **Administration > User Accounts**. The *User Accounts* page displays.

This page displays the users defined in the system.

STEP 2 Click **Add** to add a new user or click **Edit** to modify a user. The *Add (or Edit) a User Account* page displays.

STEP 3 Enter the parameters.

- **User Name**—Enter a new username between 0 and 20 characters. UTF-8 characters are not permitted.

- **Password**—Enter a password (UTF-8 characters are not permitted). If the password strength and complexity is defined, the user password must comply with the policy configured in the **Setting Password Complexity Rules** section.
- **Confirm Password**—Enter the password again.
- **Password Strength Meter**—Displays the strength of password. The policy for password strength and complexity are configured in the *Password Strength* page.

STEP 4 Click **Apply**. The user is added to the Running Configuration file of the switch.

Setting Password Complexity Rules

Setting Password Complexity Rules

Passwords are used to authenticate users accessing the switch. Simple passwords are potential security hazards. Therefore, password complexity requirements are enforced by default and may be configured as necessary. Password complexity requirements are configured on the **Password Strength** page reached through the Security drop-down menu. Additionally, password aging time may be configured on this page.

To define password complexity rules:

STEP 1 Click **Security > Password Strength**. The *Password Strength* page displays.

STEP 2 Enter the following aging parameters for passwords:

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

NOTE Password aging also applies to zero-length passwords (no password).

STEP 3 Select **Password Complexity Settings** to enable complexity rules for passwords.

If password complexity is enabled, passwords must conform to the following default settings:

- Have a minimum length of eight characters.

- Contain characters from at least three character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard).
- Are different from the current password.
- Contain no character that is repeated more than three times consecutively.
- Do not repeat or reverse the user's name or any variant reached by changing the case of the characters.
- Do not repeat or reverse the manufacturer's name or any variant reached by changing the case of the characters.

STEP 4 If the **Password Complexity Settings** are enabled, the following parameters may be configured:

- **Minimal Password Length**—Enter the minimal number of characters required for passwords.
NOTE A zero-length password (no password) is allowed, and can still have password aging assigned to it.
- **Minimal Number of Character Classes**—Enter the number of character classes which must be present in a password. Character classes are lower case (1), upper case (2), digits (3), and symbols or special characters (4).
- **The New Password Must Be Different than the Current One**—If selected, the new password cannot be the same as the current password upon a password change.

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

Configuring RADIUS Parameters

Remote Authorization Dial-In User Service (RADIUS) servers provide a centralized 802.1X or MAC-based network access control. The switch is a RADIUS client that can use a RADIUS server to provide centralized security.

For the RADIUS server to grant access to the web-based switch configuration utility, the RADIUS server must return `cisco-avpair = shell:priv-lvl=15`.

To set the RADIUS server parameters:

-
- STEP 1** Click **Security > RADIUS**. The *RADIUS* page displays.
- STEP 2** Enter the default RADIUS parameters. Values entered in the *Default Parameters* are applied to all servers. If a value is not entered for a specific server (in the *Add RADIUS Server* page) the switch uses the values in these fields.
- **IP Version**—Displays the supported IP version: IPv6 and/or IPv4 subnet.
 - **Retries**—Enter the number of transmitted requests that are sent to the RADIUS server before a failure is considered to have occurred.
 - **Timeout for Reply**—Enter the number of seconds that the switch waits for an answer from the RADIUS server before retrying the query, or switching to the next server.
 - **Dead Time**—Enter the number of minutes that elapse before a non-responsive RADIUS server is bypassed for service requests. If the value is 0, the server is not bypassed.
 - **Key String**—Enter the default key string used for authenticating and encrypting between the switch and the RADIUS server. This key must match the key configured on the RADIUS server. A key string is used to encrypt communications by using MD5. A key configured for an individual RADIUS server has precedence over the default key that is used if there is no key provided for an individual server.
- STEP 3** Click **Apply**. The RADIUS settings for the switch are updated in the Running Configuration file.

- STEP 4** To add a RADIUS server, click **Add**. The *Add RADIUS Server* page displays.
- STEP 5** Enter the values in the fields for each server. To use the default values entered in the *RADIUS* page, select **Use Default**.
- **Server Definition**—Select whether to specify the RADIUS server by IP address or name.
 - **IP Version**—If the RADIUS server will be identified by IP address, select either IPv4 or IPv6, to indicate that it will be entered in the selected format.
 - **IPv6 Address Type**—Displays that IPv6 address type is Global.
 - **Server IP Address/Name**—Enter the IP address or domain name of the server.
 - **Priority**—Enter the priority of the server. The priority determines the order the switch attempts to contact the servers to authenticate a user. The switch will start with the highest priority RADIUS server first. Zero is the highest priority.
 - **Key String**—Enter the key string used for authenticating and encrypting communication between the switch and the RADIUS server. This key must match the key configured on the RADIUS server. If this field is left blank, the switch attempts to authenticate to the RADIUS server by using the default Key String.
 - **Timeout for Reply**—Enter the number of seconds the switch waits for an answer from the RADIUS server before retrying the query, or switching to the next server. If there is no value entered in this field, the switch uses the default timeout value.
 - **Authentication Port**—Enter the UDP port number of the RADIUS server for authentication requests.
 - **Retries**—Enter the number of requests that are sent to the RADIUS server before a failure is considered to have occurred. Select **Use Default** to use the default value for the number of retries.
 - **Dead Time**—Enter the number of minutes that must pass before a non-responsive RADIUS server is bypassed for service requests. Select **Use Default** to use the default value for the dead time. If you enter 0 minutes, there is no dead time.
 - **Usage Type**—Enter the RADIUS server authentication type. The options are:
 - *Login*—RADIUS server is used for authenticating users that ask to administer the switch.

- *802.1X*—RADIUS server is used for 802.1x authentication.
- *All*—RADIUS server is used for authenticating user that ask to administer the switch and for 802.1X authentication.

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

Configuring Management Access Authentication

Authentication methods can be assigned to HTTP/HTTPS sessions. The authentication can be performed locally or on a RADIUS server.

User authentication occurs in the order that the authentication methods are selected. If the first authentication method is not available, the next selected method is used. For example, if the selected authentication methods are RADIUS and Local, and all configured RADIUS servers are queried in priority order and do not reply, the user is authenticated locally.

If an authentication method fails or the user has insufficient privilege level, the user is denied access to the switch. In other words, if authentication fails at an authentication method, the switch stops; it does not continue and does not attempt to use the next authentication method.

To define authentication methods for an access method:

STEP 1 Click **Security > Management Access Authentication**. The *Management Access Authentication* page displays.

STEP 2 Select an access method from the **Application** list.

STEP 3 Use the arrows to move the authentication method between the Optional Methods column and the Selected Methods column. The first method selected is the first method that is used.

- *RADIUS*—User is authenticated on a RADIUS server. You must have configured one or more RADIUS servers.
- *None*—User is allowed to access the switch without authentication.
- *Local*—Username and password is checked against the data stored on the local switch. These username and password pairs are defined in the *User Accounts* page.

NOTE The **Local** or **None** authentication method must always be selected last. All authentication methods selected after **Local** or **None** are ignored.

STEP 4 Click **Apply**. The selected authentication methods are associated with the access method.

Defining Access Profiles

Access profiles determine how to authenticate and authorize users accessing the switch through various access methods. Access Profiles can limit management access from specific sources.

Only users who pass both the active access profile and the management access authentication methods are given management access to the switch.

There can only be a single access profile active on the switch at one time.

Access profiles consist of one or more rules. The rules are executed in order of their priority within the access profile (top to bottom).

Rules are composed of filters that include the following elements:

- **Access Methods**—Methods for accessing and managing the switch:
 - Hypertext Transfer Protocol (HTTP)
 - Secure HTTP (HTTPS)
 - All of the above
- **Action**—Permit or deny access to an interface or source address.
- **Interface**—Which ports, LAGs, or VLANs are permitted to access or are denied access to the web-based switch configuration utility.
- **Source IP Address**—IP addresses or subnets that are allowed access.

Active Access Profile

The *Access Profiles* page displays the access profiles that are defined and enables selecting one access profile to be the active one.

When a user attempts to access the switch through an access method, the switch looks to see if the active access profile explicitly permits management access to the switch through this method. If no match is found, access is denied.

When an attempt to access the switch is in violation of the active access profile, the switch generates a SYSLOG message to alert the system administrator of the attempt.

After an access profile has been defined, additional rules can be added or edited by using the [Defining Profile Rules](#) page.

Use the *Access Profiles* page to create an access profile and to add its first rule. If the access profile only contains a single rule, you are finished. To add additional rules to the profile, use the Profile Rules page.

-
- STEP 1** Click **Security > Mgmt Access Method > Access Profiles**. The *Access Profiles* page displays.

This page displays all of the access profiles, active and inactive.

- STEP 2** To change the active access profile, select a profile from the **Active Access Profile** drop down menu and click **Apply**. This makes the chosen profile the active access profile.

NOTE Some 200 Series switches only support web access. The profile you define may be customized according to a set of settings provided in Access Profile entry, but ultimately will only provide web access; console or any other methods (SSH & Telnet) are not supported.

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

- STEP 3** Click **OK** to select the active access profile or click **Cancel** to discontinue the action.
- STEP 4** Click **Add** to open the *Add Access Profile* page. The page allows you to configure a new profile and one rule.
- STEP 5** Enter the parameters.
- **Access Profile Name**—Enter an access profile name. The access profile name can contain up to 32 characters.
 - **Rule Priority**—Enter the rule priority. When the packet is matched to a rule, user groups are either granted or denied access to the switch. The rule priority is essential to matching packets to rules, as packets are matched on a first-match basis. One is the highest priority.

- **Management Method**—Select the management method for which the rule is defined. The options are:
 - *All*—Assigns all management methods to the rule.
 - *HTTP*—Users requesting access to the switch who meet the HTTP access profile criteria, are permitted or denied.
 - *Secure HTTP (HTTPS)*—Users requesting access to the switch who meet the HTTPS access profile criteria, are permitted or denied.
- **Action**—Select the action attached to the rule. The options are:
 - *Permit*—Permits access to the switch if the user matches the settings in the profile.
 - *Deny*—Denies access to the switch if the user matches the settings in the profile.
- **Applies to Interface**—Select the interface attached to the rule. The options are:
 - *All*—Applies to all ports, VLANs, and LAGs.
 - *User Defined*—Applies to selected interface.
- **Interface**—Enter the interface number if User Defined was selected.
- **Applies to Source IP Address**—Select the type of source IP address to which the access profile applies. The *Source IP Address* field is valid for a subnetwork. Select one of the following values:
 - *All*—Applies to all types of IP addresses.
 - *User Defined*—Applies to only those types of IP addresses defined in the fields.
- **IP Version**—Select the supported IP version of the source address, IPv6 or IPv4.
- **IP Address**—Enter the source IP address.
- **Mask**—Select the format for the subnet mask for the source IP address, and enter a value in one of the fields:
 - *Network Mask*—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
 - *Prefix Length*—Select the Prefix Length and enter the number of bits that comprise the source IP address prefix.

-
- STEP 6** Click **Apply**. The access profile is created, and the Running Configuration file is updated. You can now select this access profile as the active access profile.
-

Defining Profile Rules

Access profiles can contain up to 128 rules to determine who is permitted to manage and access the switch, and the access methods that may be used.

Each rule in an access profile contains an action and a criteria (one or more parameters) to match. Each rule has a priority; rules with the lowest priority are checked first. If the incoming packet matches a rule, the action associated with the rule is performed. If no matching rule is found within the active access profile, the packet is dropped.

For example, you can limit access to the switch from all IP addresses except IP addresses that are allocated to the IT management center. In this way, the switch can still be managed and has gained another layer of security.

To add profile rules to an access profile:

-
- STEP 1** Click **Security > Mgmt Access Method > Profile Rules**. The *Profiles Rules* page displays.
- STEP 2** Select the Filter field, and an access profile. Click **Go**.
- The selected access profile is displayed in the Profile Rule Table.
- STEP 3** Click **Add** to add a rule to it. The *Add Profile Rule* page displays.
- STEP 4** Enter the parameters.
- **Access Profile Name**—Select an access profile.
 - **Rule Priority**—Enter the rule priority. When the packet is matched to a rule, user groups are either granted or denied access to the switch. The rule priority is essential to matching packets to rules, as packets are matched on a first-fit basis.
 - **Management Method**—Select the management method for which the rule is defined. The options are:
 - *All*—Assigns all management methods to the rule.

- *HTTP*—Assigns HTTP access to the rule. Users requesting access to the switch who meet the HTTP access profile criteria, are permitted or denied.
- *Secure HTTP (HTTPS)*—Users requesting access to the switch who meet the HTTPS access profile criteria, are permitted or denied.
- **Action**—Select **Permit** to permit the users that attempt to access the switch by using the configured access method from the interface and IP source defined in this rule. Or select **Deny** to deny access.
- **Applies to Interface**—Select the interface attached to the rule. The options are:
 - *All*—Applies to all ports, VLANs, and LAGs.
 - *User Defined*—Applies only to the port, VLAN, or LAG selected.
- **Interface**—Enter the interface number.
- **Applies to Source IP Address**—Select the type of source IP address to which the access profile applies. The *Source IP Address* field is valid for a subnetwork. Select one of the following values:
 - *All*—Applies to all types of IP addresses.
 - *User Defined*—Applies to only those types of IP addresses defined in the fields.
- **IP Version**—Select the supported IP version of the source address: IPv6 or IPv4.
- **IP Address**—Enter the source IP address.
- **Mask**—Select the format for the subnet mask for the source IP address, and enter a value in one of the field:
 - *Network Mask*—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
 - *Prefix Length*—Select the Prefix Length and enter the number of bits that comprise the source IP address prefix.

STEP 5 Click **Apply**, and the rule is added to the access profile.

Configuring TCP/UDP Services

The *TCP/UDP Services* page enables TCP or UDP-based services on the switch, usually for security reasons.

The switch offers the following TCP/UDP services:

- **HTTP**—Enabled by factory default
- **HTTPS**—Disabled by factory default

The active TCP connections are also displayed in this window.

To configure TCP/UDP services:

STEP 1 Click **Security > TCP/UDP Services**. The *TCP/UDP Services* page displays.

STEP 2 Enable or disable the following TCP/UDP services on the displayed services.

- **HTTP Service**—Indicates whether the HTTP service is enabled or disabled.
- **HTTPS Service**—Indicates whether the HTTPS service is enabled or disabled.

The TCP Service Table displays the following fields for each service:

- **Service Name**—Access method through which the switch is offering the TCP service.
- **Type**—IP protocol the service uses.
- **Local IP Address**—Local IP address through which the switch is offering the service.
- **Local Port**—Local TCP port through which the switch is offering the service.
- **Remote IP Address**—IP address of the remote device that is requesting the service.
- **Remote Port**—TCP port of the remote device that is requesting the service.
- **State**—Status of the service.

The UDP Services table displays the following information:

- **Service Name**—Access method through which the switch is offering the UDP service.
- **Type**—IP protocol the service uses.

- **Local IP Address**—Local IP address through which the switch is offering the service.
- **Local Port**—Local UDP port through which the switch is offering the service.
- **Application Instance**—The service instance of the UDP service. (For example, when two senders send data to the same destination.)

STEP 3 Click **Apply**. The services are added, and the Running Configuration file is updated.

Defining Storm Control

When Broadcast, Multicast, or Unknown Unicast frames are received, they are duplicated, and a copy is sent to all possible egress ports. This means that in practice they are sent to all ports belonging to the relevant VLAN. In this way, one ingress frame is turned into many, creating the potential for a traffic storm.

Storm protection enables you to limit the number of frames entering the switch and to define the types of frames that are counted towards this limit.

When a threshold is entered in the system, the port discards traffic after that threshold is reached. The port remains blocked until the traffic rate drops below this threshold. It then resumes normal forwarding.

To define Storm Control:

STEP 1 Click **Security > Storm Control**. The *Storm Control* page displays.

All the fields on this page are described in the *Edit Storm Control* page except for the **Storm Control Rate Threshold (%)**. It displays the percent of the total available bandwidth for unknown Unicast, Multicast, and Broadcast packets before storm control is applied at the port. The default value is 10% of the maximum rate of the port and is set in the *Edit Storm Control* page.

STEP 2 Select a port and click **Edit**. The *Edit Storm Control* page displays.

STEP 3 Enter the parameters.

- **Port**—Select the port for which storm control is enabled.
- **Storm Control**—Select to enable Storm Control.

- **Storm Control Rate Threshold**—Enter the maximum rate at which unknown packets can be forwarded. The default for this threshold is 10,000 for FE devices and 100,000 for GE devices.
- **Storm Control Mode**—Select one of the modes:
 - *Unknown Unicast, Multicast & Broadcast*—Counts unknown Unicast, Broadcast, and Multicast traffic towards the bandwidth threshold.
 - *Multicast & Broadcast*—Counts Broadcast and Multicast traffic towards the bandwidth threshold.
 - *Broadcast Only*—Counts only Broadcast traffic towards the bandwidth threshold.

STEP 4 Click **Apply**. Storm control is modified, and the Running Configuration file is updated.

Configuring Port Security

Network security can be increased by limiting access on a port to users with specific MAC addresses. The MAC addresses can be either dynamically learned or statically configured.

Port security monitors received and learned packets. Access to locked ports is limited to users with specific MAC addresses.

Port Security has two modes:

- **Classic Lock**—All learned MAC addresses on the port are locked, and the port does not learn any new MAC addresses. The learned addresses are not subject to aging or re-learning.
- **Limited Dynamic Lock**—The switch learns MAC addresses up to the configured limit of allowed addresses. After the limit is reached, the switch does not learn additional addresses. In this mode, the addresses are subject to aging and re-learning.

When a frame from a new MAC address is detected on a port where it is not authorized (the port is classically locked, and there is a new MAC address, or the port is dynamically locked, and the maximum number of allowed addresses has been exceeded), the protection mechanism is invoked, and one of the following actions can take place:

- Frame is discarded
- Frame is forwarded
- Port is shut down

When the secure MAC address is seen on another port, the frame is forwarded, but the MAC address is not learned on that port.

In addition to one of these actions, you can also generate traps, and limit their frequency and number to avoid overloading the devices.

NOTE Traps on the 200 Series are SYSLOG-related traps, not generated through SNMP.

NOTE If you want to use 802.1X on a port, it must be in multiple host or multi session mode. Port security on a port cannot be set if the port is in single mode (see the *802.1x, Host and Session Authentication* page).

To configure port security:

-
- STEP 1** Click **Security > Port Security**. The *Port Security* page displays.
- STEP 2** Select an interface to be modified, and click **Edit**. The *Edit Port Security Interface Settings* page displays.
- STEP 3** Enter the parameters.
- **Interface**—Select the interface name.
 - **Interface Status**—Select to lock the port.
 - **Learning Mode**—Select the type of port locking. To configure this field, the Interface Status must be unlocked. The Learning Mode field is enabled only if the *Interface Status* field is locked. To change the Learning Mode, the Lock Interface must be cleared. After the mode is changed, the Lock Interface can be reinstated. The options are:
 - *Classic Lock*—Locks the port immediately, regardless of the number of addresses that have already been learned.

- *Limited Dynamic Lock*—Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both re-learning and aging of MAC addresses are enabled.
- **Max No. of Addresses Allowed**—Enter the maximum number of MAC addresses that can be learned on the port if *Limited Dynamic Lock* learning mode is selected. The number 0 indicates that only static addresses are supported on the interface.
- **Action on Violation**—Select an action to be applied to packets arriving on a locked port. The options are:
 - *Discard*—Discards packets from any unlearned source.
 - *Forward*—Forwards packets from an unknown source without learning the MAC address.
 - *Shutdown*—Discards packets from any unlearned source, and shuts down the port. The port remains shut down until reactivated, or until the switch is rebooted.
- **Trap**—Select to enable traps when a packet is received on a locked port. This is relevant for lock violations. For Classic Lock, this is any new address received. For Limited Dynamic Lock, this is any new address that exceeds the number of allowed addresses.

NOTE Traps on the 200 Series are SYSLOG-related and not generated through SNMP.

- **Trap Frequency**—Enter minimum time (in seconds) that elapses between traps.

STEP 4 Click **Apply**. Port security is modified, and the Running Configuration file is updated.

Configuring 802.1X

Port-based access control has the effect of creating two types of access on the switch ports. One point of access enables uncontrolled communication, regardless of the authorization state (*uncontrolled port*). The other point of access authorizes communication between a host and the switch.

The 802.1x is an IEEE standard for port-based network access control. The 802.1x framework enables a device (the supplicant) to request port access from a remote device (authenticator) to which it is connected. Only when the supplicant requesting port access is authenticated and authorized is it permitted to send data to the port. Otherwise, the authenticator discards the supplicant data.

Authentication of the supplicant is performed by an external RADIUS server through the authenticator. The authenticator monitors the result of the authentication.

In the 802.1x standard, a device can be a supplicant and an authenticator at a port simultaneously, requesting port access and granting port access. However, this device is only the authenticator, and does not take on the role of a supplicant.

The following varieties of 802.1X exist:

- **Single session 802.1X:**
 - **A1**—Single-session/single host. In this mode, the switch, as an authenticator, supports a single 802.1x session and grants permission to use the port to the authorized supplicant. All access by other devices received from the same port are denied until the authorized supplicant is no longer using the port or the access is to the unauthenticated VLAN.
 - **Single session/multiple hosts**—This follows the 802.1x standard. In this mode, the switch as an authenticator allows any device to use a port as long as it has been granted permission.
- **Multi-Session 802.1X**—Every device (supplicant) connecting to a port must be authenticated and authorized by the switch (authenticator) separately in a different 802.1x session. Authentication Methods

The authentication method can be:

- **802.1x**—The switch supports the authentication mechanism as described in the standard to authenticate and authorize 802.1x supplicants.

802.1X Parameters Workflow

Define the 802.1X parameters as follows:

- (Optional) Define one or more static VLANs as unauthenticated VLANs as described in the [Defining 802.1X Properties](#) section. 802.1x authorized and unauthorized devices or ports can always send or receive packets to or from unauthenticated VLANs.

- Define 802.1X settings for each port by using the *Edit Port Authentication* page.

Note the following:

- You can select the Guest VLAN field to have untagged incoming frames go to the guest VLAN.
- Define host authentication parameters for each port using the *Port Authentication* page.
- View 802.1X authentication history using the *Authenticated Hosts* page.

Defining 802.1X Properties

The *802.1X Properties* page is used to globally enable 802.1X and define how ports will be authenticated. For 802.1X to function, it must be activated both globally and individually on each port.

To define port-based authentication:

STEP 1 Click **Security > 802.1X > Properties**. The *802.1X Properties* page displays.

STEP 2 Enter the parameters.

- **Port-Based Authentication**—Enable or disable port-based, 802.1X authentication.
- **Authentication Method**—Select the user authentication methods. The options are:
 - *RADIUS, None*—Perform port authentication first by using the RADIUS server. If no response is received from RADIUS (for example, if the server is down), then no authentication is performed, and the session is permitted.
 - *RADIUS*—Authenticate the user on the RADIUS server. If no authentication is performed, the session is not permitted.
 - *None*—Do not authenticate the user. Permit the session.

STEP 3 Click **Apply**. The 802.1X properties are modified, and the Running Configuration file is updated.

Defining 802.1X Port Authentication

The *Port Authentication* page enables configuration of 802.1X parameters for each port. Since some of the configuration changes are only possible while the port is in *Force Authorized* state, such as host authentication, it is recommended that you change the port control to *Force Authorized* before making changes. When the configuration is complete, return the port control to its previous state.

NOTE A port with 802.1x defined on it cannot become a member of a LAG.

To define 802.1X authentication:

STEP 1 Click **Security > 802.1X > Port Authentication**. The *Port Authentication* page displays.

This page displays authentication settings for all ports.

STEP 2 Select a port, and click **Edit**. The *Edit Port Authentication* page displays.

STEP 3 Enter the parameters.

- **Interface**—Select a port.
- **User Name**—Displays the username of the port.
- **Current Port Control**—Displays the current port authorization state. If the state is *Authorized*, the port is either authenticated or the *Administrative Port Control* is *Force Authorized*. Conversely, if the state is *Unauthorized*, then the port is either not authenticated or the *Administrative Port Control* is *Force Unauthorized*.
- **Administrative Port Control**—Select the Administrative Port Authorization state. The options are:
 - *Force Unauthorized*—Denies the interface access by moving the interface into the unauthorized state. The switch does not provide authentication services to the client through the interface.
 - *Auto*—Enables port-based authentication and authorization on the switch. The interface moves between an authorized or unauthorized state based on the authentication exchange between the switch and the client.
 - *Force Authorized*—Authorizes the interface without authentication.
- **Authentication Method**—Select the authentication method for the port. The options are:

- *802.1X Only*—802.1X authentication is the only authentication method performed on the port.
 - **Periodic Reauthentication**—Select to enable port re-authentication attempts after the specified Reauthentication Period.
 - **Reauthentication Period**—Enter the number of seconds after which the selected port is reauthenticated.
 - **Reauthenticate Now**—Select to enable immediate port re-authentication.
 - **Authenticator State**—Displays the defined port authorization state. The options are:
 - *Force-Authorized*—Controlled port state is set to Force-Authorized (forward traffic).
- NOTE** If the port is not in Force-Unauthorized, it is in Auto Mode and the authenticator displays the state of the authentication in progress. After the port is authenticated, the state is shown as Authenticated.
- **Quiet Period**—Enter the number of seconds that the switch remains in the quiet state following a failed authentication exchange.
 - **Resending EAP**—Enter the number of seconds that the switch waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request.
 - **Max EAP Requests**—Enter the maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout), the authentication process is restarted.
 - **Supplicant Timeout**—Enter the number of seconds that lapses before EAP requests are resent to the supplicant.
 - **Server Timeout**—Enter the number of seconds that lapses before the switch resends a request to the authentication server.
 - **Termination Cause**—Displays the reason for which the port authentication was terminated, if applicable.

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

Defining Host and Session Authentication

The *Host and Session Authentication* page enables defining the mode in which 802.1X operates on the port and the action to perform if a violation has been detected.

The 802.1X modes are:

- **Single**—Only a single authorized host can access the port. (Port Security cannot be enabled on a port in single-host mode.)
- **Multiple Host (802.1X)**—Multiple hosts can be attached to a single 802.1X-enabled port. Only the first host must be authorized, and then the port is open for all who want to access the network. If the host authentication fails, or an EAPOL-logoff message is received, all attached clients are denied access to the network.
- **Multiple Sessions**—Enables the number of specific authorized hosts to access the port. Each host is treated as if it were the first and only user and must be authenticated. Filtering is based on the source MAC address.

To define 802.1X advanced settings for ports:

STEP 1 Click **Security > 802.1X > Host and Session Authentication**. The *Host and Session Authentication* page displays.

802.1X authentication parameters are described for all ports. All fields except the following are described in the *Edit Host and Session Authentication* page.

- **Status**—Displays the host status. An asterisk indicates that the port is either not linked or is down. The options are:
 - *Unauthorized*—Either the port control is *Force Unauthorized* and the port link is down, or the port control is *Auto* but a client has not been authenticated via the port.
 - *Force-Authorized*—Clients have full port access.
 - *Single-host Lock*—Port control is *Auto* and only a single client has been authenticated by using the port.
 - *No Single Host*—Port control is *Auto* and Multiple Hosts mode is enabled. At least one client has been authenticated.
 - *Not in Auto Mode*—Auto port control is not enabled.

- **Number of Violations**—Displays the number of packets that arrive on the interface in single-host mode, from a host whose MAC address is not the supplicant MAC address.

STEP 2 Select a port, and click **Edit**. The *Edit Host and Session Authentication* page displays.

STEP 3 Enter the parameters.

- **Interface**—Enter a port number for which host authentication is enabled.
- **Host Authentication**—Select one of the modes. These modes are described above in *Defining Host and Session Authentication*.

NOTE The following fields are only relevant if you select Single in the Host Authentication field.

- **Action on a (Single Host) Violation**—Select the action to be applied to packets arriving in Single Session/Single Host mode, from a host whose MAC address is not the supplicant MAC address. The options are:
 - *Discard*—Discards the packets.
 - *Forward*—Forwards the packets.
 - *Shutdown*—Discards the packets and shuts down the port. The ports remains shut down until reactivated, or until the switch is rebooted.
- **Traps on Single Host Violation**—Select to enable traps.

NOTE Traps on the 200 Series are SYSLOG related and not SNMP related.
- **Trap Frequency (on Single Host Violation)**—Defines how often traps are sent to the host. This field can be defined only if multiple hosts are disabled.

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

Viewing Authenticated Hosts

To view details about authenticated users:

- STEP 1** Click **Security > 802.1X > Authenticated Hosts**. The *Authenticated Hosts* page displays.

This page displays the following fields:

- **User Name**—Supplicant names that were authenticated on each port.
 - **Port**—Number of the port.
 - **Session Time (DD:HH:MM:SS)**—Amount of time that the supplicant was logged on the port.
 - **Authentication Method**—Method by which the last session was authenticated. The options are:
 - *None*—No authentication is applied; it is automatically authorized.
 - *RADIUS*—Supplicant was authenticated by a RADIUS server.
 - **MAC Address**—Displays the supplicant MAC address.
- STEP 2** Click **Apply**. The settings are defined, and the Running Configuration file is updated.

Denial of Service Prevention

Denial of Service (DoS) Prevention increases network security by preventing packets with certain IP address parameters from entering the network.

SCT

The Cisco Small Business switch is an advanced switch that handles the following types of traffic, in addition to end-user traffic:

- Management traffic
- Protocol traffic
- Snooping traffic

Unwanted traffic burdens the CPU, and might prevent normal switch operation.

The switch uses the Secure Core Technology (SCT) feature, which ensures that the switch will receive and process management and protocol traffic, no matter how much total traffic is received.

SCT is enabled by default on the device and cannot be disabled.

There are no interactions with other features.

SCT can be monitored in the Denial of Service > *Security Suite Settings* page (**Details** button).

Denial of Service Security Suite Settings

NOTE Before activating DoS Prevention, you must unbind all Access Control Lists (ACLs) or advanced QoS policies that are bound to a port. ACL and advanced QoS policies are not active when a port has DoS Protection enabled on it.

To configure DoS Prevention global settings and monitor SCT:

-
- STEP 1** Click **Security > Denial of Service Prevention > Security Suite Settings**. The *Security Suite Settings* displays.
- STEP 2** **CPU Protection Mechanism: Enabled** indicates that SCT is enabled. Click **Details** beside **CPU Utilization** to enable viewing CPU resource utilization information.
-

Configuring Quality of Service

The Quality of Service feature is applied throughout the network to ensure that network traffic is prioritized according to required criteria and the desired traffic receives preferential treatment.

This section contains the following topics:

- [QoS Features and Components](#)
- [Configuring QoS - General](#)
- [Managing QoS Statistics](#)

QoS Features and Components

The QoS feature is used to optimize network performance.

QoS provides the following:

- Classification of incoming traffic to traffic classes, based on attributes, including:
 - Device Configuration
 - Ingress interface
 - Packet content
 - Combination of these attributes

QoS includes the following:

- **Traffic Classification**—Classifies each incoming packet as belonging to a specific traffic flow, based on the packet contents and/or the port. The classification is done by ACL (Access Control List), and only traffic that meets the ACL criteria is subject to CoS or QoS classification
- **Assignment to Hardware Queues**—Assigns incoming packets to forwarding queues. Packets are sent to a particular queue for handling as a function of the traffic class to which they belong.
- **Other Traffic Class-Handling Attribute**—Applies QoS mechanisms to various classes, including bandwidth management.

QoS Operation

When using the QoS feature, all traffic of the same class receives the same treatment, which consists of a single QoS action of determining the egress queue on the egress port, based on the indicated QoS value in the incoming frame. This is the VLAN Priority Tag (VPT) 802.1p value in Layer 2 and the Differentiated Service Code Point (DSCP) value for IPv4 or Traffic Class (TC) value for IPv6 in Layer 3. When operating in Basic Mode, the switch trusts this external assigned QoS value. The external assigned QoS value of a packet determines its traffic class and QoS.

The type of header field to be trusted is entered in the *Global Settings* page. For every value of that field, an egress queue is assigned, indicating through which queue the frame is sent, in the *CoS/802.1p to Queue* page or the *DSCP to Queue* page (depending on whether the trust mode is CoS/802.1p or DSCP, respectively).

QoS Workflow

To configure general QoS parameters, perform the following:

- STEP 1** Enable QoS by using the *QoS Properties* page to select the trust mode. Then enable QoS on ports by using the *Interface Settings* page.
- STEP 2** Assign each interface a default CoS or DSCP priority by using the *QoS Properties* page.
- STEP 3** Assign the schedule method (Strict Priority or WRR) and bandwidth allocation for WRR to the egress queues by using the *Queue* page.
- STEP 4** Designate an egress queue to each IP DSCP/TC value with the *DSCP to Queue* page. If the switch is in DSCP trusted mode, incoming packets are put into the egress queues based on the their DSCP/TC value.
- STEP 5** Designate an egress queue to each CoS/802.1p priority. If the switch is in CoS/802.1 trusted mode, all incoming packets will be put into the designated egress queues according to the CoS/802.1p priority in the packets. This is done by using the *CoS/802.1p to Queue* page.
- STEP 6** Enter bandwidth and rate limits in the following pages:
 - a. Set egress shaping per queue by using the *Egress Shaping Per Queue* page.
 - b. Set ingress rate limit and egress shaping rate per port by using the *Bandwidth* page.

Configuring QoS - General

The *QoS Properties Page* contains fields for enabling QoS and selecting the trust mode to be used. In addition, the default CoS priority or DSCP value for each interface can be defined.

Setting QoS Properties

To enable QoS:

- STEP 1** Click **Quality of Service > General > QoS Properties**. The *QoS Properties* page opens.
- STEP 2** Enable QoS on the switch.

STEP 3 Select a trust mode (CoS/802.1p or DSCP) and click **Apply**.

STEP 4 If you selected DSCP, proceed to **STEP 6**; if you selected CoS, proceed to the next step.

STEP 5 Select **Port/LAG** and click **GO** to display/modify all ports/LAGs and their CoS information.

The following fields are displayed for all ports/LAGs:

- **Interface**—Type of interface.
- **Default CoS**—Default VPT value for incoming packets that do not have a VLAN Tag. The default CoS is 0. The default is only relevant for untagged frames if *Trust CoS* is selected.

Select **Restore Defaults** to restore the factory CoS default setting for this interface.

STEP 6 Click **DSCP Override Table** to enter the DSCP values. The *DSCP Override Table* opens.

STEP 7 DSCP In displays the DSCP value of the incoming packet that needs to be re-marked to an alternative value. Select the new DSCP value to override the incoming value.

Select Restore Defaults to restore the factory DSCP values.

STEP 8 Click **Apply**. The Running Configuration file is updated.

To set QoS on an interface, select it, and click **Edit**. The *Edit Interface CoS Configuration* page opens.

STEP 1 Enter the parameters.

- **Interface**—Select the port or LAG.
- **Default CoS**—Select the default CoS (Class-of-Service) value to be assigned for incoming packets (that do not have a VLAN tag). The range is 0-7.

STEP 2 Click **Apply**. The interface default CoS value is set, and the Running Configuration file is updated.

Interface QoS Settings

The *Interface Settings* page enables configuring QoS on each port of the switch, as follows:

QoS State Disabled on an Interface—All inbound traffic on the port is mapped to the best effort queue and no classification/prioritization takes place.

QoS State of the Port is Enabled—Port prioritize traffic on ingress is based on the system wide configured trusted mode, which is either CoS/802.1p trusted mode or DSCP trusted mode.

To enter QoS settings per interface:

-
- STEP 1** Click **Quality of Service > General > Interface Settings**. The *Interface Settings* page opens.
 - STEP 2** Select **Port** or **LAG** to display the list of ports or LAGs.

The list of ports/LAGs is displayed. **QoS State** displays whether QoS is enabled on the interface.
 - STEP 3** Select an interface, and click **Edit**. The *Edit QoS Interface Settings* opens.
 - STEP 4** Select **the Port** or **LAG** interface.
 - STEP 5** Click to enable or disable **QoS State** for this interface.
 - STEP 6** Click **Apply**. The Running Configuration file is updated.
-

Configuring QoS Queues

The switch supports four queues for each interface. Queue number four is the highest priority queue. Queue number one is the lowest priority queue.

There are two ways of determining how traffic in queues is handled, Strict Priority and Weighted Round Robin (WRR).

Strict Priority—Egress traffic from the highest-priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, thus providing the highest level of priority of traffic to the highest numbered queue.

Weighted Round Robin (WRR)—In WRR mode the number of packets sent from the queue is proportional to the weight of the queue (the higher the weight the more frames are sent). For example, if all four queues are WRR and the default weights are used, queue 1 receives 1/15 of the bandwidth (assuming all queues are saturated and there is congestion), queue 2 receives 2/15, queue 3 receives 4/15 and queue 4 receives 8/15 of the bandwidth. The type of WRR algorithm used in the device is not the standard Deficit WRR (DWRR), but rather Shaped Deficit WRR (SDWRR).

The queuing modes can be selected in the *Queue* page. When the queuing mode is by strict priority, the priority sets the order in which queues are serviced, starting with queue_4 (the highest priority queue) and going to the next lower queue when each queue is completed.

When the queuing mode is Weighted Round Robin, queues are serviced until their quota has been used up and then another queue is serviced.

It is also possible to assign some of the lower queues to WRR, while keeping some of the higher queues in strict priority. In this case traffic for the strict priority queues is always sent before traffic from the WRR queues. Only after the strict priority queues have been emptied is traffic from the WRR queues forwarded. (The relative portion from each WRR queue depends on its weight).

To select the priority method and enter WRR data.

STEP 1 Click **Quality of Service > General > Queue**. The *Queue* page opens.

STEP 2 Enter the parameters.

- **Queue**—Displays the queue number.
- **Scheduling Method:** Select one of the following options:
 - *Strict Priority*—Traffic scheduling for the selected queue and all higher queues is based strictly on the queue priority.
 - *WRR*—Traffic scheduling for the selected queue is based on WRR. The period time is divided between the WRR queues that are not empty, meaning they have descriptors to egress. This happens only if strict priority queues are empty.
 - *WRR Weight*—If WRR is selected, enter the WRR weight assigned to the queue.
 - *% of WRR Bandwidth*—Displays the amount of bandwidth assigned to the queue. These values represent the percent of the WRR weight.

- STEP 3** Click **Apply**. The queues are configured, and the Running Configuration file is updated.

Mapping CoS/802.1p to a Queue

The *CoS/802.1p to Queue* page maps 802.1p priorities to egress queues. The CoS/802.1p to Queue Table determines the egress queues of the incoming packets based on the 802.1p priority in their VLAN Tags. For incoming untagged packets, the 802.1p priority will be the default CoS/802.1p priority assigned to the ingress ports.

Default Mapping Queues

802.1p Values (0-7, 7 being the highest)	Queue (4 queues 1-4, 4 being the highest priority)	Queue (2 queues: Normal and High)	Notes
0	1	Normal	Background
1	1	Normal	Best Effort
2	2	Normal	Excellent Effort
3	3	Normal	Critical Application LVS phone SIP
4	3	Normal	Video
5	4	High	Voice Cisco IP phone default
6	4	High	Interwork Control LVS phone RTP
7	4	High	Network Control

By changing the CoS/802.1p to Queue mapping and the Queue schedule method and bandwidth allocation, it is possible to achieve the desired quality of services in a network.

CoS/802.1p to Queue mapping is applicable only if CoS/802.1p is the trusted mode and the packets belong to flows that are CoS trusted.

Queue 1 has the lowest priority, queue 4 has the highest priority.

To map CoS values to egress queues:

-
- STEP 1** Click **Quality of Service > General > CoS/802.1p to Queue**. The *CoS/802.1p to Queue* page opens.
- STEP 2** Enter the parameters.
- **802.1p**—Displays the 802.1p priority tag values to be assigned to an egress queue, where 0 is the lowest and 7 is the highest priority.
 - **Output Queue**—Select the egress queue to which the 802.1p priority is mapped. Four egress queues are supported, where Queue 4 is the highest priority egress queue and Queue 1 is the lowest priority.
- STEP 3** For each 802.1p priority, select the Output Queue to which it is mapped.
- STEP 4** Click **Apply**. 801.1p priority values to queues are mapped, and the Running Configuration file is updated.
-

Mapping DSCP to Queue

The DSCP (IP *Differentiated Services Code Point*) to Queue page maps DSCP to egress queues. The DSCP to Queue Table determines the egress queues of the incoming IP packets based on their DSCP values. The original VPT (VLAN Priority Tag) of the packet is unchanged.

By simply changing the DSCP to Queue mapping and the Queue schedule method and bandwidth allocation, it is possible to achieve the desired quality of services in a network.

DSCP to Queue mapping is applicable to IP packets if DSCP is the trusted mode.

Non-IP packets are always classified to the best-effort queue

To map DSCP to queues:

STEP 1 Click **Quality of Service > General > DSCP to Queue**. The *DSCP to Queue* page opens.

The *DSCP to Queue* page contains **Ingress DSCP**. It displays the DSCP value in the incoming packet and its associated class.

STEP 2 Select the **Output Queue** (traffic forwarding queue) to which the DSCP value is mapped.

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

Configuring Bandwidth

The *Bandwidth* page enables network managers to define two sets of values, Ingress Rate Limit and Egress Shaping Rate, that determine how much traffic the system can receive and send.

The ingress rate limit is the number of bits per second that can be received from the ingress interface. Excess bandwidth above this limit is discarded.

The following values are entered for egress shaping:

- Committed Information Rate (CIR) sets the average maximum amount of data allowed to be sent on the egress interface, measured in bits per second
- Committed Burst Size (CBS) is the burst of data that is allowed to be sent, even though it is above the CIR. This is defined in number of bytes of data.

To enter bandwidth limitation:

STEP 1 Click **Quality of Service > General > Bandwidth**. The *Bandwidth* page opens.

The *Bandwidth* page displays bandwidth information for each interface.

The % column is the ingress rate limit for the port divided by the total port bandwidth.

STEP 2 Select an interface, and click **Edit**. The *Edit Bandwidth* page opens.

STEP 3 Select the **Port or LAG** interface.

STEP 4 Enter the fields for the selected interface:

- **Ingress Rate Limit**—Select to enable the ingress rate limit, which is defined in the field below.
- **Ingress Rate Limit**—Enter the maximum amount of bandwidth allowed on the interface.

NOTE The two **Ingress Rate Limit** fields do not appear when the interface type is LAG.

- **Egress Shaping Rate**—Select to enable egress shaping on the interface.
- **Committed Information Rate (CIR)**—Enter the maximum bandwidth for the egress interface.
- **Committed Burst Size (CBS)**—Enter the maximum burst size of data for the egress interface in bytes of data. This amount can be sent even if it temporarily increases the bandwidth beyond the allowed limit.

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

Configuring Egress Shaping per Queue

In addition to limiting transmission rate per port, which is done in the *Bandwidth* page, the switch can limit the transmission rate of selected egressing frames on a per-queue per-port basis. Egress rate limiting is performed by shaping the output load.

The switch limits all frames except for management frames. Any frames that are not limited are ignored in the rate calculations, meaning that their size is not included in the limit total.

Per-queue Egress rate shaping can be disabled.

To define egress shaping per queue:

STEP 1 Click **Quality of Service > General > Egress Shaping per Queue**. The *Egress Shaping Per Queue* page opens.

The *Egress Shaping Per Queue* page displays the rate limit and burst size for each queue.

STEP 2 Select an interface type (Port or LAG), and click **Go**. The list of Ports/LAGs is displayed.

STEP 3 Select a Port/LAG, and click **Edit**. The *Edit Egress Shaping Per Queue* page opens.

This page enables shaping the egress for up to four queues on each interface.

STEP 4 Select the **Interface**.

STEP 5 For each queue that is required, enter the following fields:

- **Enable Shaping**—Select to enable egress shaping on this queue.
- **Committed Information Rate (CIR)**—Enter the maximum rate (CIR) in Kbits per second (Kbps). CIR is the average maximum amount of data that can be sent.
- **Committed Burst Size (CBS)**—Enter the maximum burst size (CBS) in bytes. CBS is the maximum burst of data allowed to be sent even if a burst exceeds CIR.

STEP 6 Click **Apply**. The bandwidth settings are modified, and the Running Configuration file is updated.

Workflow to Configure Basic QoS Mode

Managing QoS Statistics

From this page you can manage the Single Policer, Aggregated Policer, and view queues statistics.

Viewing Policer Statistics

A Single Policer is bound to a class map from a single policy. An Aggregate Policer is bound to one or more class maps from one or more policies.

Viewing Queues Statistics

The *Queues Statistics* page displays queue statistics, including statistics of forwarded and dropped packets, based on interface, queue, and drop precedence.

NOTE QoS Statistics are shown only when the switch is in QoS Advanced Mode only. This change is made in **General > QoS Properties**.

To view Queues Statistics:

STEP 1 Click **Quality of Service > QoS Statistics > Queues Statistics**. The *Queues Statistics* page opens.

This page displays the following fields:

- **Refresh Rate**—Select the time period that passes before the interface Ethernet statistics are refreshed. The available options are:
 - *No Refresh*—Statistics are not refreshed.
 - *15 Sec*—Statistics are refreshed every 15 seconds.
 - *30 Sec*—Statistics are refreshed every 30 seconds.
 - *60 Sec*—Statistics are refreshed every 60 seconds.
- **Counter Set**—The options are:
 - *Set 1*—Displays the statistics for Set 1 that contains all interfaces and queues with a high DP (Drop Precedence).
 - *Set 2*—Displays the statistics for Set 2 that contains all interfaces and queues with a low DP.
- **Interface**—Queue statistics are displayed for this interface.
- **Queue**—Packets were forwarded or tail dropped from this queue.
- **Drop Precedence**—Lowest drop precedence has the lowest probability of being dropped.
- **Total packets**—Number of packets forwarded or tail dropped.
- **Tail Drop packets**—Percentage of packets that were tail dropped.

STEP 2 Click **Add**. The *Add Queues Statistics* page opens.

STEP 3 Enter the parameters.

-
- **Counter Set**—Select the counter set:
 - *Set 1*—Displays the statistics for Set 1 that contains all interfaces and queues with a high DP (Drop Precedence).
 - *Set 2*—Displays the statistics for Set 2 that contains all interfaces and queues with a low DP.
 - **Interface**—Select the ports for which statistics are displayed. The options are:
 - *Port*—Selects the port on the selected unit number for which statistics are displayed.
 - *All Ports*—Specifies that statistics are displayed for all ports.
 - **Queue**—Select the queue for which statistics are displayed.
 - **Drop Precedence**—Enter drop precedence that indicates the probability of being dropped.
- STEP 4** Click **Apply**. The Queue Statistics counter is added, and the Running Configuration file is updated.
-

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)