ADMINISTRATION GUIDE

Cisco Small Business 300 Series Managed Switch Administration Guide Release 1.3.5

Table of Contents

Chapter 1: Getting Started 1

Starting the Web-based Configuration Utility 1

Quick Start Device Configuration 4

Interface Naming Conventions 5

/Window Navigation 7

Chapter 2: Status and Statistics 11

System Summary 11

Viewing Ethernet Interfaces 11

Viewing Etherlike Statistics 13

Viewing 802.1X EAP Statistics 14

Health 15

Managing RMON 15

View Log 23

Chapter 3: Administration: System Log 24

Setting System Log Settings 24

Setting Remote Logging Settings 26

Viewing Memory Logs 28

Chapter 4: Administration: File Management 30

System Files 30

Upgrade/Backup Firmware/Language 33

Download/Backup Configuration/Log 37

Configuration Files Properties 42

Copy/Save Configuration 43

Auto Configuration via DHCP 44

Chapter 5: Administration 51

Device Models 51
System Settings 53
Management Interface 55
User Accounts 55
Defining Idle Session Timeout 55
Time Settings 56
System Log 56
File Management 56
Rebooting the Device 56
Health 58
Diagnostics 59
Discovery - Bonjour 59
Discovery - LLDP 59
Discovery - CDP 60
Ping 60

Chapter 6: Administration: Time Settings 62

System Time Options 63
SNTP Modes 64
Configuring System Time 65

Chapter 7: Administration: Diagnostics 73

Testing Copper Ports 73
Displaying Optical Module Status 75
Configuring Port and VLAN Mirroring 77
Viewing CPU Utilization and Secure Core Technology 78

Chapter 8: Administration: Discovery 80

Bonjour 80

LLDP and CDP 81
Configuring LLDP 82
Configuring CDP 102

Chapter 9: Administration: Unidirectional Link Detection 112
UDLD Overview 112
UDLD Operation 113
Usage Guidelines 116
Dependencies On Other Features 116
Default Settings and Configuration 117
Before You Start 117
Common UDLD Tasks 117
Configuring UDLD 118

Chapter 10: Port Management 122
Configuring Ports 122
Setting Port Configuration 123
Link Aggregation 127
PoE 134
Configuring Green Ethernet 134

Chapter 11: Smartport 143
Overview 143
What is a Smartport 144
Smartport Types 144
Smartport Macros 147
Macro Failure and the Reset Operation 148
How the Smartport Feature Works 149
Auto Smartport 149
Error Handling 153

Default Configuration 153
Relationships with Other Features and Backwards Compatibility 154
Common Smartport Tasks 154
Configuring Smartport Using The Web-based Interface 156
Built-in Smartport Macros 161

Chapter 12: Port Management: PoE 174

PoE on the Device 174
Configuring PoE Properties 177
Configuring PoE Settings 178

Chapter 13: VLAN Management 181

VLANs 181
Configuring Default VLAN Settings 184
Creating VLANs 185
Configuring VLAN Interface Settings 186
Defining VLAN Membership 187
Voice VLAN 190

Chapter 14: Spanning Tree 204

STP Flavors 204
Configuring STP Status and Global Settings 205
Defining Spanning Tree Interface Settings 207
Configuring Rapid Spanning Tree Settings 209

Chapter 15: Managing MAC Address Tables 212

Configuring Static MAC Addresses 213
Managing Dynamic MAC Addresses 214

Chapter 16: Multicast 216

Multicast Forwarding 216

Defining Multicast Properties 219
Adding MAC Group Address 220
Adding IP Multicast Group Addresses 222
Configuring IGMP Snooping 224
MLD Snooping 226
Querying IGMP/MLD IP Multicast Group 228
Defining Multicast Router Ports 229
Defining Forward All Multicast 230
Defining Unregistered Multicast Settings 231

Chapter 17: IP Configuration 234

Overview 234
IPv4 Management and Interfaces 236
Domain Name 250

Chapter 18: Security 256

Defining Users 257
Configuring RADIUS 260
264
Management Access Method 264
Management Access Authentication 269
Secure Sensitive Data Management 270
SSL Server 270
SSH Client 272
Configuring TCP/UDP Services 273
Defining Storm Control 274
Configuring Port Security 275
802.1X 278
Denial of Service Prevention 278

Chapter 19: Security: 802.1X Authentication 282

Overview of 802.1X 282

Authenticator Overview 284

Common Tasks 288

802.1X Configuration Through the GUI 289

Chapter 20: Security: First Hop Security 296

First Hop Security Overview 297

Router Advertisement Guard 301

Neighbor Discovery Inspection 301

DHCPv6 Guard 302

Neighbor Binding Integrity 303

Attack Protection 305

Policies, Global Parameters and System Defaults 307

Common Tasks 308

Default Settings and Configuration 310

Before You Start 311

Configuring First Hop Security through Web GUI 311

Chapter 21: Security: Secure Sensitive Data Management 323

Introduction 323

SSD Rules 324

SSD Properties 329

Configuration Files 332

SSD Management Channels 337

Menu CLI and Password Recovery 337

Configuring SSD 338

Chapter 22: Security: SSH Client 341

Secure Copy (SCP) and SSH 341

Protection Methods 342
SSH Server Authentication 344
SSH Client Authentication 345
Before You Begin 346
Common Tasks 346
SSH Client Configuration Through the GUI 348

Chapter 23: Security: SSH Server 352
Overview 352
Common Tasks 353
SSH Server Configuration Pages 354

Chapter 24: Access Control 358
Access Control Lists 358
Defining MAC-based ACLs 360
IPv4-based ACLs 363
IPv6-Based ACLs 367
Defining ACL Binding 371

Chapter 25: Quality of Service 373
QoS Features and Components 374
Configuring QoS - General 375
Managing QoS Statistics 384

Chapter 26: SNMP 387
SNMP Versions and Workflow 387
Model OIDs 390
SNMP Engine ID 391
Configuring SNMP Views 393
Creating SNMP Groups 394

Managing SNMP Users 396
Defining SNMP Communities 398
Defining Trap Settings 400
Notification Recipients 400
SNMP Notification Filters 405

1

Getting Started

This section provides an introduction to the web-based configuration utility, and covers the following topics:

- **Starting the Web-based Configuration Utility**
- **Quick Start Device Configuration**
- **Interface Naming Conventions**
- **Window Navigation**

Starting the Web-based 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

If you are using IPv6 interfaces on your management station, use the IPv6 global address and not the IPv6 link local address to access the device from your browser.

Launching the Configuration Utility

To open the web-based configuration utility:

STEP 1 Open a Web browser.

STEP 2 Enter the IP address of the device you are configuring in the address bar on the browser, and then press **Enter**.

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

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.

NOTE If you have not previously selected a language for the GUI, the language of the Login page is determined by the language(s) requested by your browser and the languages configured on your device. If your browser requests Chinese, for example, and Chinese has been loaded into your device, the Login page is automatically displayed in Chinese. If Chinese has not been loaded into your device, the Login page appears in English.

The languages loaded into the device have a language and country code (en-US, en-GB and so on). For the Login page to be automatically displayed in a particular language, based on the browser request, both the language and country code of the browser request must match those of the language loaded on the device. If the browser request contains only the language code without a country code (for example: fr). The first embedded language with a matching language code is taken (without matching the country code, for example: fr_CA).

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 device 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 appears. 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 appears.

If you entered an incorrect username or password, an error message appears 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 log on to the system. If you select this option, the System Summary page is opened instead of the Getting Started page.

HTTP/HTTPS

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

NOTE There is no need to input the username/password prior to clicking the **Secure Browsing (HTTPS)** button**.**

For information on how to configure HTTPS, see **SSL Server**.

Password Expiration

The New Password page appears:

- The first time you access the device 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

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

CAUTION Unless the Running Configuration is copied to the Startup Configuration, rebooting the device will remove all changes made since the last time the file was saved. 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 to the left of the **Save** application link indicates that Running

Configuration changes 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 device auto-discovers a device, such as an IP phone (see **What is a Smartport**), and 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 you log on even though you did not make any configuration changes.

When you click **Save**, the Copy/Save Configuration page appears. 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 device.

When a timeout occurs or you intentionally log out of the system, a message appears and the Login page appears, 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 Device Configuration

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

Category	Link Name (on the Page)	Linked Page
	Change Management Applications and Services	TCP/UDP Services page
	Change Device IP Address	IPv4 Interface page
	Create VLAN	Create VLAN page
	Configure Port Settings	Port Setting page
Device Status	System Summary	System Summary page
	Port Statistics	Interface page
	RMON Statistics	Statistics page
	View Log	RAM Memory page
Quick Access	Change Device Password	User Accounts page
	Upgrade Device Software	Upgrade/Backup Firmware/ Language page
	Backup Device Configuration	Download/Backup Configuration/Log page
	Create MAC Based ACL	MAC Based ACL page
	Create IP Based ACL	IPv4 Based ACL page
	Configure QoS	QoS Properties page
	Configure Port Mirroring	Port and VLAN Mirroring page

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

Interface Naming Conventions

Within the GUI, interfaces are denoted by concatenating the following elements:

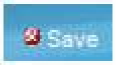
- **Type of interface:** The following types of interfaces are found on the various types of devices:
  - **Fast Ethernet (10/100 bits)**—These are displayed as **FE**.
  - **Gigabit Ethernet ports (10/100/1000 bits)**—These are displayed as **GE**.
  - **LAG (Port Channel)**—These are displayed as **LAG**.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

Window Navigation

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

Application Header

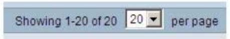
The Application Header appears on every page. It provides the following application links:

Application Link Name	Description
	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. Click **Save** to display the Copy/Save Configuration page. Save the Running Configuration file by copying it to the Startup Configuration file type on the device. After this save, the red X icon and the Save application link are no longer displayed. When the device is rebooted, it copies the Startup Configuration file type to the Running Configuration and sets the device parameters according to the data in the Running Configuration.
Username	Displays the name of the user logged on to the device. The default username is **cisco**. (The default password is **cisco**).

Application Link Name	Description
Language Menu	This menu provides the following options: - **Select a language:** Select one of the languages that appear in the menu. This language will be the web-based configuration utility language. - **Download Language:** Add a new language to the device. - **Delete Language:** Deletes the second language on the device. The first language (English) cannot be deleted. - **Debug:** Used for translation purposes. If you select this option, all web-based configuration utility labels disappear and in their place are the IDs of the strings that correspond to the IDs in the language file. **NOTE** To upgrade a language file, use the Upgrade/Backup Firmware/Language page.
Logout	Click to log out of the web-based switch configuration utility.
About	Click to display the device name and device version number.
Help	Click to display the online help.
⊗ Alert	The SYSLOG Alert Status icon appears when a SYSLOG message, above the *critical* severity level, is logged. Click the icon to open the RAM Memory page. After you access this page, the SYSLOG Alert Status icon is no longer displayed. To display the page when there is not an active SYSLOG message, Click **Status and Statistics** > **View Log** > **RAM Memory**.

Management Buttons

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

Button Name	Description
 Showing 1-20 of 20 20 per page	Use the pull-down menu to configure the number of entries per page.
✱	Indicates a mandatory field.
Add	Click to display the related Add page and add an entry to a table. Enter the information and click **Apply** to save it to the Running Configuration. Click **Close** to return to the main page. Click **Save** to display the Copy/Save Configuration page and save the Running Configuration to the Startup Configuration file type on the device.
Apply	Click to apply changes to the Running Configuration on the device. If the device is rebooted, the Running Configuration is lost, unless it is saved to the Startup Configuration file type or another file type. Click **Save** to display the Copy/Save Configuration page and save the Running Configuration to the Startup Configuration file type on the device.
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 any changes were not applied to the Running Configuration, a message appears.

Button Name	Description
Copy Settings	A table typically contains one or more entries containing configuration settings. Instead of modifying each entry individually, it is possible to modify one entry and then copy the selected entry to multiple entries, as described below: 1. Select the entry to be copied. Click **Copy Settings** to display the popup. 2. Enter the destination entry numbers in the **to** field. 3. Click **Apply** to save the changes and click **Close** to return to the main page.
Delete	After selecting an entry in the table, click **Delete** to remove.
Details	Click to display the details associated with the entry selected.
Edit	Select the entry and click **Edit**. The Edit page appears, and the entry can be modified. 1. Click **Apply** to save the changes to the Running Configuration. 2. Click **Close** to return to the main page.
Go	Enter the query filtering criteria and click **Go**. The results are displayed on the page.
Refresh	Clich **Refresh** to refresh the counter values.
Test	Click **Test** to perform the related tests.

2

Status and Statistics

This section describes how to view device statistics.

It covers the following topics:

- **System Summary**
- **Viewing Ethernet Interfaces**
- **Viewing Etherlike Statistics**
- **<300-500>Viewing GVRP Statistics**
- **Viewing 802.1X EAP Statistics**
- **<300-500>Viewing TCAM Utilization**
- **Health**
- **Managing RMON**
- **View Log**

System Summary

See **System Settings**.

Viewing Ethernet Interfaces

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 and/or set the refresh rate:

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

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 or view statistics counters:

- Click **Clear Interface Counters** to clear counters for the interface displayed.
- Click **View All Interfaces Statistics** to see all ports on a single page.

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 and/or set the refresh rate:

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

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—**Frames that were 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 rejected due to excessive collisions.
- **Oversize Packets—**Packets greater than 2000 octets received.
- **Internal MAC Receive Errors—**Frames rejected because of receiver errors.
- **Pause Frames Received—**Received flow control pause frames.
- **Pause Frames Transmitted—**Flow control pause frames transmitted from the selected interface.

To clear statistics counters:

- Click **Clear Interface Counters** to clear the selected interfaces counters.

- Click **View All Interfaces Statistics** to see all ports on a single page.

Viewing GVRP Statistics

The GVRP page displays information regarding GARP VLAN Registration Protocol (GVRP) frames that were sent or received from a port. GVRP is a standards-based Layer 2 network protocol, for automatic configuration of VLAN information on switches. It was defined in the 802.1ak amendment to 802.1Q-2005.

GVRP statistics for a port are only displayed if GVRP is enabled globally and on the port. See the GVRP page.

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

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

STEP 2 Enter the parameters.

- **Interface**—Select the specific interface for which GVRP statistics are to be displayed.
- **Refresh Rate**—Select the time period that passes before the GVRP statistics page is refreshed.

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

- **Join Empty**—Number of GVRP Join Empty packets received/transmitted.
- **Empty**—Number of GVRP empty packets received/transmitted.
- **Leave Empty**—Number of GVRP Leave Empty packets received/transmitted.
- **Join In**—Number of GVRP Join In packets received/transmitted.
- **Leave In**—Number of GVRP Leave In packets received/transmitted.
- **Leave All**—Number of GVRP Leave All packets received/transmitted.

The GVRP Error Statistics section displays the GVRP error counters.

- **Invalid Protocol ID**—Invalid protocol ID errors.
- **Invalid Attribute Type**—Invalid attribute ID errors.

- **Invalid Attribute Value—**Invalid attribute value errors.
- **Invalid Attribute Length—**Invalid attribute length errors.
- **Invalid Event—**Invalid events.

To clear statistics counters:

- Click **Clear Interface Counters** to clear the selected counters.
- Click **View All Interfaces Statistics** to see all ports on a single page.

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 and/or set the refresh rate:

STEP 1 Click **Status and Statistics** > **802.1x EAP**.

STEP 2 Select the **Interface** 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 statistics counters:

- Click **Clear Interface Counters** to clear the selected interfaces counters.
- Click **Clear All Interface Counters** to clear the counters of all interfaces.

Viewing TCAM Utilization

The device architecture uses a Ternary Content Addressable Memory (TCAM) to support packet actions in wire speed.

TCAM holds the rules produced by applications, such as ACLs (Access Control Lists), Quality of Service (QoS), IP Routing and user-created rules.

Some applications allocate rules upon their initiation. Additionally, processes that initialize during system boot use some of their rules during the startup process.

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

The TCAM Utilization page shows the following fields:

- **Maximum TCAM Entries for IPv4 and Non-IP (Rules)**—Maximum TCAM Entries available.
- **IPv4 Routing**
  - **In Use**—Number of TCAM entries used for IPv4 routing.

  - **Maximum—**Number of available TCAM entries that can be used for IPv4 routing.

- **Non-IP Rules**
  - **In Use—**Number of TCAM entries used for non-IP rules.
  - **Maximum—**Number of available TCAM entries that can be used for non-IP rules.

Health

See **Health**.

Managing RMON

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

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

With this feature, you can perform the following actions:

- View the current statistics (since the counter values were cleared). You can also collect the values of these counters over a period of time, and then view the table of collected data, where each collected set is a single line of the *History* tab.
- Define interesting changes in counter values, such as “reached a certain number of late collisions” (defines the alarm), and then specify what action to perform when this event occurs (log, trap, or log and trap).

Viewing RMON Statistics

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

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

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

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

STEP 2 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**—Number of octets received, including bad packets and FCS octets, but excluding framing bits.
- **Drop Events**—Number of packets 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 2000 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.
  - Received (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 of 1024 Bytes or More—**Number of frames, containing 1024-2000 bytes, and Jumbo Frames, that were received.

To clear statistics counters:

- Click **Clear Interface Counters** to clear the selected interfaces counters.
- Click **View All Interfaces Statistics** to see all ports on a single page.

Configuring RMON History

The RMON feature enables monitoring statistics per interface.

The History Control Table page defines the sampling frequency, amount of samples to store and the port from where to gather the data.

After the data is sampled and stored, it appears in the History Table page that can be viewed by clicking **History Table**.

To enter RMON control information:

STEP 1 Click **Status and Statistics > RMON > History**. The fields displayed on this page are defined in the Add RMON History page, below. The only field is that is on this page and not defined in the Add page is:

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

STEP 2 Click **Add**.

STEP 3 Enter the parameters.

- **New History Entry**—Displays the number of the new History table entry.
- **Source Interface**—Select the type of interface from which the history samples are to be taken.
- **Max No. of Samples to Keep**—Enter the number of samples to store.
- **Sampling Interval**—Enter the time in seconds that samples are collected from the ports. The field range is 1-3600.
- **Owner**—Enter the RMON station or user that requested the RMON information.

STEP 4 Click **Apply**. The entry is added to the History Control Table page, and the Running Configuration file is updated.

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

Viewing the RMON History Table

The History Table page displays interface-specific statistical network samplings. The samples were configured in the History Control table described above.

To view RMON history statistics:

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

STEP 2 Click **History Table**.

STEP 3 From the **History Entry No.** list, select the entry number of the sample to display.

The fields are displayed for the selected sample.

- **Owner**—History table entry owner.
- **Sample No.**—Statistics were taken from this sample.
- **Drop Events**—Dropped packets due to lack of network resources during the sampling interval. This may not represent the exact number of dropped packets, but rather the number of times dropped packets were detected.
- **Bytes Received**—Octets received including bad packets and FCS octets, but excluding framing bits.
- **Packets Received**—Packets received, including bad packets, Multicast, and Broadcast packets.
- **Broadcast Packets**—Good Broadcast packets excluding Multicast packets.
- **Multicast Packets**—Good Multicast packets received.
- **CRC Align Errors**—CRC and Align errors that have occurred.
- **Undersize Packets**—Undersized packets (less than 64 octets) received.
- **Oversize Packets**—Oversized packets (over 2000 octets) received.
- **Fragments**—Fragments (packets with less than 64 octets) received, excluding framing bits, but including FCS octets.
- **Jabbers**—Total number of received packets that were longer than 2000 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.
- **Collisions**—Collisions received.
- **Utilization**—Percentage of current interface traffic compared to maximum traffic that the interface can handle.

Defining RMON Events Control

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

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

To define RMON events:

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

This page displays previously defined events.

STEP 2 Click **Add.**

STEP 3 Enter the parameters.

- **Event Entry**—Displays the event entry index number for the new entry.
- **Community**—Enter the SNMP community string to be included when traps are sent (optional). Note that the community must be defined using the **Defining SNMPv1,2 Notification Recipients** or **Defining SNMPv3 Notification Recipients** pages for the trap to reach the Network Management Station.
- **Description**—Enter a name for the event. This name is used in the Add RMON Alarm page to attach an alarm to an event.
- **Notification Type**—Select the type of action that results from this event. Values are:
    - *None*—No action occurs when the alarm goes off.
    - *Log (Event Log Table)*—Add a log entry to the Event Log table when the alarm is triggered.
    - *Trap (SNMP Manager and SYSLOG Server)*—Send a trap to the remote log server when the alarm goes off.
    - *Log and Trap*—Add a log entry to the Event Log table and send a trap to the remote log server when the alarm goes off.
- **Time—**Displays the time of the event. (This is a read-only table in the parent window and cannot be defined).
- **Owner—**Enter the device or user that defined the event.

STEP 4 Click **Apply**. The RMON event is saved to the Running Configuration file.

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

Viewing the RMON Events Logs

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

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

STEP 2 Click **Event Log Table**.

This page displays the following fields:

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

Defining RMON Alarms

RMON alarms provide a mechanism for setting thresholds and sampling intervals to generate exception events on any counter or any other SNMP object counter maintained by the agent. Both the rising and falling thresholds must be configured in the alarm. After a rising threshold is crossed, no rising events are generated until the companion falling threshold is crossed. After a falling alarm is issued, the next alarm is issued when a rising threshold is crossed.

One or more alarms are bound to an event, which indicates the action to be taken when the alarm occurs.

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

To enter RMON alarms:

STEP 1 Click **Status and Statistics > RMON** > **Alarms**. All previously-defined alarms are displayed. The fields are described in the Add RMON Alarm page below. In addition to those fields, the following field appears:

- Counter Value—Displays the value of the statistic during the last sampling period.

STEP 2 Click **Add.**

STEP 3 Enter the parameters.

- **Alarm Entry**—Displays the alarm entry number.
- **Interface**—Select the type of interface for which RMON statistics are displayed.
- **Counter Name**—Select the MIB variable that indicates the type of occurrence measured.
- **Sample Type**—Select the sampling method to generate an alarm. The options are:
  - *Absolute*—If the threshold is crossed, an alarm is generated.
  - *Delta*—Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold. If the threshold was crossed, an alarm is generated.
- **Rising Threshold**—Enter the value that triggers the rising threshold alarm.
- **Rising Event**—Select an event to be performed when a rising event is triggered. Events are created in the Events page.
- **Falling Threshold**—Enter the value that triggers the falling threshold alarm.
- **Falling Event**—Select an event to be performed when a falling event is triggered.
- **Startup Alarm**—Select the first event from which to start generation of alarms. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
  - *Rising Alarm*—A rising value triggers the rising threshold alarm.
  - *Falling Alarm*—A falling value triggers the falling threshold alarm.
  - *Rising and Falling*—Both rising and falling values trigger the alarm.

- **Interval—**Enter the alarm interval time in seconds.
- **Owner—**Enter the name of the user or network management system that receives the alarm.

STEP 4 Click **Apply**. The RMON alarm is saved to the Running Configuration file.

View Log

See **Viewing Memory Logs**.

3

Administration: System Log

This section describes the System Log feature, which enables the device to generate multiple independent logs. Each log is a set of messages describing system events.

The device generates the following local logs:

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

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

This section covers the following sections:

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

Setting System Log Settings

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

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

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

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

STEP 2 Enter the parameters.

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

- **Originator Identifier**—Enables adding an origin identifier to SYSLOG messages. The options are:
  - *None*—Do not include the origin identifier in SYSLOG messages.
  - *Hostname*—Include the system hostname in SYSLOG messages.
  - *IPv4 Address*—Include the IPv4 address of the sending interface in SYSLOG messages.
  - *IPv6 Address*—Include the IPv6 address of the sending interface in SYSLOG messages.
  - *User Defined*—Enter a description to be included in SYSLOG messages.
- **RAM Memory Logging**—Select the severity levels of the messages to be logged to the RAM.
- **Flash Memory Logging**—Select the severity levels of the messages to be logged to the Flash memory.

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

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**.

STEP 2 Enter the following fields:

- IPv4 Source Interface—Select the source interface whose IPv4 address will be used as the source IPv4 address of SYSLOG messages sent to SYSLOG servers.
- IPv6 Source Interface—Select the source interface whose IPv6 address will be used as the source IPv6 address of SYSLOG messages sent to SYSLOG servers.

NOTE If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

STEP 3 Click **Add**.

STEP 4 Enter the parameters.

- **Server Definition—**Select whether to identify the remote log server by IP address or name.
- **IP Version—**Select the supported IP format.
- **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 5 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 device can write to the following logs:

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

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

RAM Memory

The RAM Memory page displays all messages that were saved in the RAM (cache) in chronological order. 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 top of the page has a button that allows you to Disable Alert Icon Blinking. **Click** to toggle between disable and enable.

This page contains 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

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

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

This page contains the following fields:

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

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

4

Administration: File Management

This section describes how system files are managed.

The following topics are covered:

- **System Files**
- **Upgrade/Backup Firmware/Language**
- **Active Image <300-500>**
- **Download/Backup Configuration/Log**
- **Configuration Files Properties**
- **Copy/Save Configuration**
- **Auto Configuration via DHCP**

System Files

System files are files that contain configuration information, firmware images or boot code.

Various actions can be performed with these files, such as: selecting the firmware file from which the device boots, copying various types of configuration files internally on the device, or copying files to or from an external device, such as an external server.

The possible methods of file transfer are:

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

Configuration files on the device are defined by their *type*, and contain the settings and parameter values for the device.

When a configuration is referenced on the device, it is referenced by its *configuration file type (such as Startup Configuration or Running Configuration)*, as opposed to a file name that can be modified by the user.

Content can be copied from one configuration 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 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 device:

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

  If the device is rebooted, the Running Configuration is lost. The Startup Configuration, stored in Flash, overwrites the Running Configuration, stored in RAM.

  To preserve any changes you made to the device, you must save the Running Configuration to the Startup Configuration, or another file type.

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

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

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

  - The device has been operating continuously for 24 hours.

  - No configuration changes have been made to the Running Configuration in the previous 24 hours.

  - The Startup Configuration is identical to the Running Configuration.

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

The option of automatically copying the Running Configuration to the mirror configuration can be disabled in the Configuration Files Properties page.

- **Backup Configuration—**A manual copy of a configuration file used 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.
- **Firmware—**The program that controls the operations and functionality of the device. More commonly referred to as the *image*.
- **Boot Code—**Controls the basic system startup and launches the firmware image.
- **Language File—**The dictionary that enables the web-based configuration utility 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 second language, as described in **Upgrade/Backup Firmware/Language** section.
- View the firmware image currently in use or select the image to be used in the next reboot as described in the **Active Image <300-500>** section.
- Save configuration files on the device to a location on another device as described in the **Download/Backup Configuration/Log** section.
- Clear the Startup Configuration or Backup Configuration file types as described in the **Configuration Files Properties** section.
- Copy one configuration file type to another configuration file type as described in the **Copy/Save Configuration** section.
- Enable automatically uploading a configuration file from a DHCP server to the device, as described in the **Auto Configuration via DHCP** section.

This section covers the following topics:

- **Upgrade/Backup Firmware/Language**
- **Active Image <300-500>**
- **Download/Backup Configuration/Log**
- **Configuration Files Properties**
- **Copy/Save Configuration**
- **Auto Configuration via DHCP**

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 or upgrade a second language file.

The following methods for transferring files are supported:

- HTTP/HTTPS that uses the facilities provided by the browser
- TFTP that requires a TFTP server
- Secure Copy Protocol (SCP) that requires an SCP server

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

There are two firmware images stored on the device. One of the images is identified as the *active image* and other image is identified as the *inactive image*.

When you upgrade the firmware, the new image always replaces the image identified as the inactive image.

Even after uploading new firmware on the device, the device continues to boot by using the active image (the old version) until you change the status of the new image to be the active image by using the procedure in the **Active Image <300-500>** section. Then boot the device.

Upgrade/Backing Firmware or Language File

To upgrade or backup a software image or language file:

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

STEP 2 Click the Transfer Method. Proceed as follows:

- If you selected TFTP, go to **STEP 3**.
- If you selected **via** HTTP/HTTPS, go to **STEP 4**.
- If you selected **via** SCP, go to **STEP 5**.

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

Select one of the following **Save Actions**:

- **Upgrade—**Specifies that the file type on the device is to be replaced with a new version of that file type located on a TFTP server.
- **Backup—**Specifies that a copy of the file type is to be saved to a file on another device.

Enter the following fields:

- **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).
- **TFTP Server Definition—**Select whether to specify the TFTP server by IP address or domain name.
- **IP Version—**Select whether an IPv4 or an IPv6 address is used.
- **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 is used) from the list.
- **TFTP Server IP Address/Name**—Enter the IP address or the domain name of the TFTP server.
- **(For Upgrade) Source File Name**—Enter the name of the source file.
- **(For Backup) Destination File Name**—Enter the name of the backup file.

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

- **File Type**—Select one of the following file types:
  - *Firmware Image*—Select this to upgrade the firmware image.
  - *Language*—Select this to upgrade the language file.
- **File Name**—Click **Browse** to select a file or enter the path and source file name to be used in the transfer.

STEP 5 If you selected via **SCP (Over SSH),** see **SSH Client Authentication** for instructions. Then, enter the following fields: (only unique fields are described, for non-unique fields, see the descriptions above)

- **Remote SSH Server Authentication**—To enable SSH server authentication (which is disabled by default), click **Edit**. This takes you to the **SSH Server Authentication** page to configure the SSH server, and return to this page. Use the **SSH Server Authentication** page to select an SSH user authentication method (password or public/private key), set a username and password on the device (if the password method is selected), and generate an RSA or DSA key if required.

SSH Client Authentication—Client authentication can be done in one of the following ways:

- **Use SSH Client System Credentials—**Sets permanent SSH user credentials. Click **System Credentials** to go to the SSH User Authentication page where the user/password can be set once for all future use.
- **Use SSH Client One-Time Credentials—**Enter the following:
  - *Username*—Enter a username for this copy action.
  - *Password*—Enter a password for this copy.

NOTE The username and password for one-time credential will not saved in configuration file.

Select one of the following **Save Actions**:

- **Upgrade**—Specifies that the file type on the device is to be replaced with a new version of that file type located on a TFTP server.
- **Backup**—Specifies that a copy of the file type is to be saved to a file on another device.

Enter the following fields:

- **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).
- **SCP Server Definition**—Select whether to specify the SCP server by IP address or by domain name.
- **IP Version**—Select whether an IPv4 or an IPv6 address is used.
- **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.
- **Link-Local Interface**—Select the link local interface from the list.
- **SCP Server IP Address/Name**—Enter the IP address or domain name of the SCP server.
- **(For Upgrade) Source File Name—**Enter the name of the source file.
- **(For Backup) Destination File Name—**Enter the name of the backup file.

STEP 6 Click **Apply**. If the files, passwords and server addresses are correct, one of the following may happen:

- If SSH server authentication is enabled (in the SSH Server Authentication page), and the SCP server is trusted, the operation succeeds. If the SCP server is not trusted, the operation fails and an error is displayed.

- If SSH server authentication is not enabled, the operation succeeds for any SCP server.

Active Image

There are two firmware images stored on the device. One of the images is identified as the *active image* and other image is identified as the *inactive image*. The device boots from the image you set as the *active image*. You can change the image identified as the *inactive image* to the *active image*. (You can reboot the device by using the process described in the **Management Interface<print only>** section).

To select the active image:

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

The page displays the following:

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

STEP 2 Select the image from the **Active Image After Reboot** menu to identify the firmware image that is used as the active image after the device is rebooted. The **Active Image Version Number After Reboot** displays the firmware version of the active image that is used after the device is rebooted.

STEP 3 Click **Apply**. The active image selection is updated.

Download/Backup Configuration/Log

The Download/Backup Configuration/Log page enables:

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

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 *overwrites* 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 device must be rebooted for the restored Startup Configuration to be used as the Running Configuration. You can reboot the device by using the process described in the **Management Interface** section.

Configuration File Backwards Compatibility

When restoring configuration files from an external device to the device, the following compatibility issues might arise:

- **Change the System Mode—**If the System mode is contained in a configuration file that is downloaded to the device, and the file's System mode matches the current System mode, this information is ignored. Otherwise, if the System mode is changed, the following cases are possible:
    - If the configuration file is downloaded onto the device (using the Download/Backup Configuration/Log page), the operation is aborted, and a message is displayed indicating that the System mode must be changed in the System Settings page.
    - If the configuration file is downloaded during an automatic configuration process, the Startup Configuration file is deleted and the device reboots automatically in the new System mode. The device is configured with an empty configuration file. See **Auto Configuration via DHCP**.

Downloading or Backing-up a Configuration or Log File

To backup or restore the system configuration file:

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

STEP 2 Select the **Transfer Method**.

STEP 3 If you selected **via 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 replaces a file type on the device. 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 /), cannot start with a period (.), and must include 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.

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

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

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

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

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

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

g. **Sensitive Data**—Select how sensitive data should be included in the backup file. The following options are available:

   - *Exclude*—Do not include sensitive data in the backup.
   - *Encrypted*—Include sensitive data in the backup in its encrypted form.
   - *Plaintext*—Include sensitive data in the backup in its plaintext form.

   NOTE The available sensitive data options are determined by the current user SSD rules. For details, refer to Secure Sensitive Data Management > SSD Rules page.

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

i. Click **Apply**. The file is upgraded or backed up.

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

Select the **Save Action**.

If **Save Action** is *Download* (replacing the file on the device with a new version from 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 device.

If **Save Action** is *Backup* (copying a file to 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. **Sensitive Data**—Select how sensitive data should be included in the backup file. The following options are available:

  - *Exclude*—Do not include sensitive data in the backup.
  - *Encrypted*—Include sensitive data in the backup in its encrypted form.
  - *Plaintext*—Include sensitive data in the backup in its plaintext form.

  NOTE The available sensitive data options are determined by the current user SSD rules. For details, refer to Secure Sensitive Data Management > SSD Rules page.

c. Click **Apply**. The file is upgraded or backed up.

STEP 5 If you selected via **SCP (Over SSH)**, see **SSH Client Configuration Through the GUI** for instructions. Then enter the following fields:

- **Remote SSH Server Authentication**—To enable SSH server authentication (it is disabled by default), click **Edit**, which takes you to the **SSH Server Authentication** page to configure this, and return to this page. Use the **SSH Server Authentication** page to select an SSH user authentication method (password or public/private key), set a username and password on the device, if the password method is selected, and generate an RSA or DSA key if required.

SSH Client Authentication—Client authentication can be done in one of the following ways:

- **Use SSH Client**—Sets permanent SSH user credentials. Click **System Credentials** to go to the SSH User Authentication page where the user/ password can be set once for all future use.
- Use SSH Client One-Time Credentials—Enter the following:
    - *Username*—Enter a username for this copy action.
    - *Password*—Enter a password for this copy.
- **SCP Server Definition—**Select whether to specify the TFTP server by IP address or by domain name.
- **IP Version**—Select whether an IPv4 or an IPv6 address is used.
- **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.
- **Link-Local Interface—**Select the link local interface from the list.
- **SCP Server IP Address/Name—**Enter the IP address or domain name of the TFTP server.

If **Save Action** is *Download* (replacing the file on the device with a new version from another device), enter the following fields.

- Source File Name—Enter the name of the source file.
- 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).

If **Save Action** is *Backup* (copying a file to another device), enter the following fields (in addition to those fields listed above):

- **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).
- **Sensitive Data**—Select how sensitive data should be included in the backup file. The following options are available:
    - *Exclude*—Do not include sensitive data in the backup.
    - *Encrypted*—Include sensitive data in the backup in its encrypted form.
    - *Plaintext*—Include sensitive data in the backup in its plaintext form.

  NOTE The available sensitive data options are determined by the current user SSD rules. For details, refer to Secure Sensitive Data Management > SSD Rules page.
- **Destination File Name**—Name of file being copied to.

STEP 6 Click **Apply**. The file is upgraded or backed up.

Configuration Files Properties

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

ITo set whether mirror configuration files will be created, clear configuration files and see when configuration files were created:

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

This page displays the following fields:

- **Configuration File Name—**Type of system file.
- **Creation Time—**Date and time that file was modified.

STEP 2 If required, disable **Auto Mirror Configuration**. This disables the automatic creation of mirror configuration files. When disabling this feature, the mirror configuration file, if it exists, is deleted. See **System Files** for a description of mirror files and why you might not want to automatically create mirror configuration files.

STEP 3 If required, select either the Startup Configuration, Backup Configuration or both and click **Clear Files** to delete these files.

Copy/Save Configuration

When you click **Apply** on any window, changes that you made to the device 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 on another device.

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

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

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

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

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

- If you are backing up a configuration file, select one of the following formats for the backup file.
  - **Exclude**—Sensitive data is not included in the backup file.
  - **Encrypted**—Sensitive data is included in the backup file in encrypted form.
  - **Plaintext**—Sensitive data is included in the backup file in plain text.

  NOTE The available sensitive data options are determined by the current user SSD rules. For details, refer to Secure Sensitive Data Management > SSD Rules page.

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

STEP 5 Click **Apply**. The file is copied.

Auto Configuration via DHCP

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

To use this feature, the device must be configured as a DHCPv4 client in which case auto configuration from a DHCPv4 server is supported and/or a DHCPv6 client in which case auto configuration from a DHCPv6 server is supported.

By default, the device is enabled as a DHCP client when the Auto Configuration via DHCP feature is enabled.

The Auto Configuration process also supports downloading a configuration file that includes sensitive information, such as RADIUS server keys and SSH/SSL keys, by using the Secured Copy Protocol (SCP) and the Secure Sensitive Data (SSD) feature (See **Security: Secure Sensitive Data Management**).

Auto Configuration via DHCPv4 is triggered in the following cases:

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

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

- When a DHCPv6 server sends information to the device. This occurs in the following cases:
  - When an interface, which is IPv6 enabled, is defined as a DHCPv6 stateless configuration client.
  - When DHCPv6 messages are received from the server (for example, when you press the **Restart** button on IPv6 Interfaces page,
  - When DHCPv6 information is refreshed by the device.
  - After rebooting the device when stateless DHCPv6 client is enabled.
- When the DHCPv6 server packets contain the configuration filename option.

DHCP Server Options

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

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

Auto Configuration Download Protocol (TFTP or SCP)

The Auto Configuration download protocol can be configured, as follows:

- **Auto By File Extension**—(Default) If this option is selected, a user-defined file extension indicates that files with this extension are downloaded using SCP (over SSH), while files with other extensions are downloaded using TFTP. For example, if the file extension specified is*.xyz*, files with the *.xyz* extension are downloaded using SCP, and files with the other extensions are downloaded using TFTP.
- **TFTP Only**—The download is done through TFTP regardless of the file extension of the configuration file name.
- **SCP Only**—The download is done through SCP (over SSH) regardless of the file extension of the configuration file name.

SSH Client Authentication Parameters

By default, remote SSH server authentication is disabled, so that the device accepts any remote SSH server out of the box. You can enable remote SSH server authentication to only allow connections from servers found in the trusted server list.

SSH Client Authentication parameters are required to access the SSH server by the client (which is the device). The default SSH Client authentication parameters are:

- SSH Authentication method: by username/password
- SSH username: anonymous
- SSH password: anonymous

NOTE The SSH Client authentication parameters can also be used when downloading a file for manual download (a download that is not performed through the DHCP Auto Configuration feature).

Auto Configuration Process

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

- The DHCP server is accessed to acquire the TFTP/SCP server name/ address and configuration file name/path (DHCPv4 options: 66,150, and 67, DHCPv6 options: 59 and 60).
- If a server and configuration file options were not supplied by the DHCP server, then:
  - **For DHCPv4:** The user-defined, backup configuration file name is used.
  - **For DHCPv6:** The process is halted.
- If the DHCP server did not send these options and the backup TFTP/SCP server address parameter is empty then:
  - **For DHCPv4:**

    SCP—The Auto Configuration process is halted.

    TFTP—The device sends TFTP Request messages to a limited Broadcast address (for IPv4) or ALL NODES address (for IPv6) on its IP interfaces and continues the process of Auto Configuration with the first answering TFTP server.
  - **For DHCPv6:** The Auto Configuration process is halted.
- If the configuration filename was supplied by the DHCP server (DHCPv4: option 67, DHCPv6: option 60), then the copy protocol (SCP/TFTP) is selected as described in **Auto Configuration Download Protocol (TFTP or SCP)**.
- When downloading using SCP, the device accepts any specified SCP/SSH server (without authentication) if either of the following is true:
  - The SSH server authentication process is disabled. Note that by default the SSH server authentication is disabled in order to allow downloading configuration file for devices with factory default configuration (for example out-of-box devices).
  - The SSH Server is configured in the SSH Trusted Servers list.

  If the SSH server authentication process is enabled, and the SSH server is not found in the SSH Trusted Servers list, the Auto Configuration process is halted.

- If the information is available, the TFTP/SCP server is accessed to download the file from it.

  The download process is done only if the new configuration filename is different from the current configuration filename (even if the current configuration file is empty).

- A SYSLOG message is generated acknowledging that the Auto Configuration process is completed.

Configuring DHCP Auto Configuration

Workflow

To configure DHCP Auto Configuration.

1. Configure the DHCPv4 and/or DHCPv6 servers to send the required options. this process is not described in this guide.
2. Configure Auto Configuration parameters.
3. Define the device as a DHCPv4 client in the **Defining an IPv4 Interface <300-500>in Layer 2 System Mode** or **Defining IPv4 Interface in Layer 3 System Mode <300-500>** pages, and/or define the device as a DHCPv6 client in the **IPv6 Interface** page.

Web Configuration

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

- Enable the DHCP auto configuration feature.
- Specify the download protocol.
- Configure the device to receive configuration information from a specific file on a specific server.

Note the following regarding the DHCP auto configuration process:

- A configuration file that is placed on the TFTP/SCP server must match the form and format requirements of the supported configuration file. The form and format of the file are checked, but the validity of the configuration *parameters* is not checked prior to loading it to the Startup Configuration.
- In IPv4, to ensure that the device configuration functions as intended, due to allocation of different IP addresses with each DHCP renew cycle, it is recommended that IP addresses 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 auto configuration:

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

STEP 2 Enter the values.

- **Auto Configuration Via DHCP**—Select this field to enable DHCP Auto Configuration. This feature is enabled by default, but can be disabled here.
- **Download Protocol—**Select one of the following options:
  - *Auto By File Extension*—Select to indicate that auto configuration uses the TFTP or SCP protocol depending on the extension of the configuration file. If this option is selected, the extension of the configuration file does not necessarily have to be given. If it is not given, the default extension is used (as indicated below).
  - *File Extension for SCP*—If **Auto By File Extension** is selected, you can indicate a file extension here. Any file with this extension is downloaded using SCP. If no extension is entered, the default file extension**.scp** is used.
  - *TFTP Only*—Select to indicate that only the TFTP protocol is to be used for auto configuration.
  - *SCP Only*—Select to indicate that only the SCP protocol is to be used for auto configuration.
- **SSH Settings for SCP—**When using SCP for downloading the configuration files, select one of the following options:
  - *Remote SSH Server Authentication*—Click on the **Enable/Disable** link to navigate to the SSH Server Authentication page. There you can enable authentication of the SSH server to be used for the download and enter the trusted SSH server if required.
  - *SSH Client Authentication*—Click on the System Credentials link to enter user credentials in the SSH User Authentication page.

STEP 3 Enter the following optional information to be used if no configuration file name was received from the DHCP server.

- **Backup Server Definition—**Select **By IP address** or **By name** to configure the server.

- **IP Version**—Select whether an IPv4 or an IPv6 address is used.
- **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 is used) from the list.
- **Backup Server IP Address/Name—**Enter the IP address or the name of the server to be used if no server IP address was specified in the DHCP message.
- **Backup Configuration File Name**—Enter the path and file name of the file to be used if no configuration file name was specified in the DHCP message.

STEP 4 Click **Apply**. The parameters are copied to the Running Configuration file.

5

Administration

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

It covers the following topics:

- **Device Models**
- **System Settings**
- **Console Settings (Autobaud Rate Support)**
- **Management Interface**
- **User Accounts**
- **Defining Idle Session Timeout**
- **Time Settings**
- **System Log**
- **File Management**
- **Routing Resources<300-500>**
- **Health**
- **Diagnostics**
- **Discovery - Bonjour**
- **Discovery - LLDP**
- **Discovery - CDP**
- **Ping**
- **Traceroute**

Device Models

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

In Layer 2 system mode, the device forwards packets as a VLAN-aware bridge. In Layer 3 system mode, the device performs both IPv4 routing and VLAN-aware bridging.

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

NOTE The following port conventions are used:

- GE is used for Gigabit Ethernet (10/100/1000) ports.
- FE is used for Fast Ethernet (10/100) ports.

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

Model Name	Product ID (PID)	Description of Ports on Device	Power Dedicated to PoE	No. of Ports that Support PoE
SG300-10	SRW2008-K9	8 GE ports, and 2 special-purpose combo ports (GE/SFP)	N/A	N/A
SG300-10MP	SRW2008MP-K9	8 GE ports, and 2 special-purpose combo ports (GE/SFP)	124W	8
SG300-10P	SRW2008P-K9	8 GE ports, and 2 special-purpose combo ports (GE/SFP)	62W	8
SG300-20	SRW2016-K9	16 GE ports, and 4 special purpose ports - 2 uplinks and 2 combo ports	N/A	N/A
SG300-28	SRW2024-K9	24 GE ports, and 4 special-purpose ports - 2 uplinks and 2 combo-ports	N/A	N/A
SG300-28P	SRW2024P-K9	24 GE ports, and 4 special-purpose ports - 2 uplinks and 2 combo-ports.	180W	24
SG300-52	SRW2048-K9	48 GE ports, and 4 special-purpose ports - 2 uplinks and 2 combo-ports	N/A	N/A
SF300-08	SRW208-K9	8 FE ports.	N/A	N/A

Model Name	Product ID (PID)	Description of Ports on Device	Power Dedicated to PoE	No. of Ports that Support PoE
SF302-08	SRW208G-K9	8 FE ports plus 2 GE ports	N/A	N/A
SF302-08MP	SRW208MP-K9	8 FE ports plus 2 GE ports	124W	8
SF302-08P	SRW208P-K9	8 FE ports plus 2 GE ports	62W	8
SG300-10PP	SG300-10PP-K9	8-Port 10/100 PoE Managed Switch	62W	8
SG300-10MPP	SG300-10MPP-K9	10-Port Gigabit PoE Managed Switch	124W	8
SF300-24	SRW224G4-K9	24 FE ports plus 4 GE special-purpose ports - 2 uplinks and 2 combo-ports.	N/A	N/A
SF300-24P	SRW224G4P-K9	24 FE ports plus 4 GE special-purpose ports - 2 uplinks and 2 combo-ports.	180W	24
SF300-24PP	SF300-24PP-K9	24-Port 10/100 PoE Managed Switch	180W	24
SG300-28PP	SG300-28PP-K9	28-Port Gigabit PoE Managed Switch	180W	24
SF300-48	SRW248G4-K9	48 FE ports plus 4 GE special-purpose ports - 2 uplinks and 2 combo-ports	N/A	N/A
SF300-48P	SRW248G4P-K9	48 FE ports plus 4 GE special-purpose ports - 2 uplinks and 2 combo-ports	375W	48
SF300-48PP	SF300-48PP-K9	48-Port 10/100 PoE Managed Switch	375W	48
SG300-52MP	SG300-52MP-K9	52-Port Gigabit PoE Managed Switch	740W	48
SG300-10SFP	SG300-10SFP-K9	10-Port Gigabit Managed SFP Switch	N/A	N/A
SF300-24MP	SF300-24M-K9	24-Port 10/100 PoE Managed Switch	375W	24
SG300-28MP	SRW2024P-K9	28-Port Gigabit PoE Managed Switch	375W	24

Model Name	Product ID (PID)	Description of Ports on Device	Power Dedicated to PoE	No. of Ports that Support PoE
SF302-08PP		8-Port 10/100 PoE Managed Switch	62W	8
SF302-08MPP		8-Port 10/100 PoE Managed Switch	124W	8
ESW2-350G-52	ESW2-350G-52-K9	52-Port Gigabit Managed Switch	N/A	N/A
ESW2-350G-52DC	ESW2-350G-52DC-K9	52-Port Gigabit Managed Switch	N/A	N/A

System Settings

The System Summary page provides a graphic view of the device, and displays device status, hardware information, firmware version information, general PoE status, and other items.

Displaying the System Summary

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

The System Summary page contains system and hardware information.

System Information:

- **System Description—**A description of the system.
- **System Location—**Physical location of the device. 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 device. Click **Edit** to go the System Settings page to enter this value. By default, the device hostname is composed of the word *device* concatenated with the three least significant bytes of the device 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**—Device MAC address.
- **Jumbo Frames**—Jumbo frame support status. This support can be enabled or disabled by using the Port Settings page of the Port Management menu.

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

TCP/UDP Services Status:

- **HTTP Service**—Displays whether HTTP is enabled/disabled.
- **HTTPS Service**—Displays whether HTTPS is enabled/disabled.
- **SNMP Service**—Displays whether SNMP is enabled/disabled.
- **Telnet Service**—Displays whether Telnet is enabled/disabled.
- **SSH Service**—Displays whether SSH is enabled/disabled.

Other Summary Information:

- **Model Description**—Device model description.
- **Serial Number**—Serial number.
- **PID VID**—Part number and version ID.
- **Firmware Version (Active Image)**—Firmware version number of the active image.
- **Firmware MD5 Checksum (Active Image)**—MD5 checksum of the active image.
- **Firmware Version (Non-active Image)**—Firmware version number of the non-active image.
- **Firmware MD5 Checksum (Non-active Image)**—MD5 checksum of the non-active 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.

PoE Power Information:

- **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.

System Settings

To enter system settings:

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

STEP 2 View or modify the system settings.

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

  NOTE If you change the system mode after clicking **Apply**, the system will require a reboot, and the startup configuration file will be gone after the boot.

  - *L2*—Select to place the device in Layer 2 system mode.
  - *L3*—Select to place the device in Layer 3 system mode.

- **Custom Banner Settings—**The following banners can be set:
  - **Login Banner—**Enter text to display on the Login page before login. Click **Preview** to view the results.
  - **Welcome Banner—**Enter text to display on the Login page after login. Click **Preview** to view the results.

NOTE When you define a login banner from the web-based configuration utility, it also activates the banner for the CLI interfaces (Console, Telnet, and SSH).

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

Console Settings (Autobaud Rate Support)

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

Auto Detection enables the device to detect your console speed automatically, so that you are not required to set it explicitly.

When Auto Detection is not enabled, the console port speed is automatically set to the last speed that was set manually at (115,200 by default).

When Auto Detection is enabled but the console baud-rate was not yet discovered, the system uses speed 115,200 for displaying text (for example, the boot-up information).

After Auto Detection is enabled in the Console Settings page, it can be activated by connecting the console to the device and press the Enter key twice. The device detects the baud rate automatically.

To enable Auto Detection or to manually set the baud rate of the console:

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

STEP 2 Select one of the following:

- Auto Detection—The console baud rate is detected automatically.
- Static—Select one of the available speeds.

Management Interface

See **IPv4 Management and Interfaces**.

User Accounts

See **Defining Users**.

Defining Idle Session Timeout

The *Idle Session Timeout* configures the time intervals that the management sessions can remain idle before they timeout and you must log in again to reestablish one of the following sessions:

- **HTTP Session Timeout**
- **HTTPS Session Timeout**
- **Console Session Timeout**
- **Telnet Session Timeout**
- **SSH Session Timeout**

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

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

STEP 2 Select the timeout for the each session from the corresponding list. The default timeout value is 10 minutes.

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

Time Settings

See **Administration: Time Settings**.

System Log

See **Administration: System Log**.

File Management

See **Administration: File Management**.

Rebooting the Device

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

You can back up the configuration by using *Administration > File Management > Copy/Save Configuration* or clicking **Save** at the top of the window. You can also upload the configuration from a remote device. See the **Download/Backup Configuration/Log** section.

There are cases when you might prefer to set the time of the reboot for some time in the future. This could happen for example in one of the following cases:

- You are performing actions on a remote device, and these actions might create loss of connectivity to the remote device. Pre-scheduling a reboot restores the working configuration and enables restoring the connectivity to the remote device. If these actions are successful, the delayed reboot can be cancelled.
- Reloading the device cause loss of connectivity in the network, thus by using delayed reboot, you can schedule the reboot to a time that is more convenient for the users (e.g. late night).

To reboot the device:

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

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

- **Reboot**—Reboots the device. Since any unsaved information in the Running Configuration is discarded when the device 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.

  The following options are available:

  - *Immediate*—Reboot immediately.
  - *Date*—Enter the date (month/day) and time (hour and minutes) of the schedule reboot. This schedules a reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 days.

    NOTE This option can only be used if the system time has either been set manually or by SNTP.

  - *In*—Reboot within the specified number of hours and minutes. The maximum amount of time that can pass is 24 days.

- **Reboot to Factory Defaults**—Reboots the device by using the factory default configuration. This process erases the Startup Configuration file and the backup configuration file.

  The mirror configuration file is not deleted when restoring to factory defaults.

- **Clear Startup Configuration File**—Check to clear the startup configuration on the device for the next time it boots up.

  NOTE Clearing the Startup Configuration File and Rebooting is not the same as Rebooting to Factory Defaults. Rebooting to Factory Defaults is more intrusive.

Routing Resources

Use the Router Resources page to display TCAM allocation and modify total TCAM size. TCAM entries are divided into the following groups:

- **IP Entries**—TCAM entries reserved for IP static routes, IP addresses on the device, and IP hosts. Each type generates the following number of TCAM entries:
  - IPv4 static routes—One entry per route
  - IP Addresses—Two entries per IP address
  - IP Hosts—One entry per host
- **Non-IP Entries**—TCAM entries reserved for other applications, such as ACL rules, CoS policers, and VLAN rate limits.

To view and modify router resources:

STEP 1 Click **Administration** > **Router Resources**.

The following fields are displayed:

- **Neighbors**—**Count** is the number of neighbors recorded on the device and **TCAM Entries** is the total number of TCAM entries being used for neighbors.
- **Interfaces**—**Count** is the number of IP addresses on interfaces on the device and **TCAM Entries** is the total number of TCAM entries being used for the IP addresses.
- **Routes**—**Count** is the number of routes recorded on the device and **TCAM Entries** is the total number of TCAM entries being used for the routes.
- **Total**—Displays the number of TCAM entries which are currently being used.
- **Maximum Entries**—Select one of the following options:
  - *Use Default*—The number of TCAM entries available for IP entries is 25% of the TCAM size.
  - *User Defined*—Enter a value.

You must save your current configuration before changing the TCAM Allocation Settings.

NOTE A summary of the TCAM entries actually in use and available is displayed at the bottom of this page. For an explanation of the fields, see **<300-500>Viewing TCAM Utilization**.

STEP 2 Save the new settings by clicking **Apply**. This checks the feasibility of the TCAM allocation. If it is incorrect, an error message is displayed. If it is correct, the allocation is saved to the Running Configuration file and a reboot is performed.

Health

The Health page monitors the fan status on all devices with fans. Depending on the model, there are one or more fans on a device. Some models have no fans at all.

On devices on which a temperature sensor is assembled, for protecting the device hardware in case it overheats, the following actions are performed by the device if it overheats and during the cool down period after overheating:

Event	Action
At least one temperature sensor exceeds the Warning threshold	The following are generated: ▪ SYSLOG message ▪ SNMP trap
At least one temperature sensor exceeds the Critical threshold	The following are generated: ▪ SYSLOG message ▪ SNMP trap The following actions are performed: ▪ System LED is set to solid amber (if hardware supports this). ▪ Disable Ports — When the Critical temperature has been exceeded for two minutes, all ports will be shut down. ▪ (On devices that support PoE) Disable the PoE circuitry so that less power is consumed and less heat is emitted.

Event	Action
Cool down period after the Critical threshold was exceeded (all sensors are lower than the Warning threshold - 2 °C).	After all the sensors cool down to Warning Threshold minus 2 degree C, the PHY will be re-enabled, and all ports brought back up. If FAN status is OK, the ports are enabled. (On devices that support PoE) the PoE circuitry is enabled.

To view the device health parameters, click **Status and Statistics** > **Health**.

The Health page displays the following fields:

- **Fan Status—**Fan status. The following values are possible:
    - OK—Fan is operating normally.
    - Fail—Fan is not operating correctly.
    - N/A—Fan ID is not applicable for the specific model.
- **Fan Direction—**(On relevant devices) The direction that the fans are working in (for example: Front to Back).

Diagnostics

See **Administration: Diagnostics**.

Discovery - Bonjour

See **Bonjour**.

Discovery - LLDP

See **Configuring LLDP**.

Discovery - CDP

See **Configuring CDP**.

Ping

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 device 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**.

STEP 2 Configure ping by entering the fields:

- **Host Definition**—Select whether to specify the source interface by its IP address or name. This field influences the interfaces that are displayed in the Source IP field, as described below.
- **IP Version**—If the source interface is identified by its IP address, select either IPv4 or IPv6 to indicate that it will be entered in the selected format.
- **Source IP**—Select the source interface whose IPv4 address will be used as the source IPv4 address for communication with the destination. If the Host Definition field was By Name, all IPv4 and IPv6 addresses will be displayed in this drop-down field. If the Host Definition field was By IP Address, only the existing IP addresses of the type specified in the IP Version field will be displayed.

  NOTE If the Auto option is selected, the system computes the source address based on the destination address.
- **Destination IPv6 Address Type**—Select Link Local or Global as the type of IPv6 address to enter as the destination IP address.

  - *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.
- **Destination 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 the number of times configured in the "Number of Pings" field, whether the ping succeeds or not. Choose to use the default interval or specify your own value.
- **Number of Pings—**The number of times the ping operation is 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 appears 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.

Traceroute

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

STEP 1 Click **Administration > Traceroute**.

STEP 2 Configure Traceroute by entering information into the following fields:

- **Host Definition—**Select whether hosts are identified 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.
- **Source IP—**Select the source interface whose IPv4 address will be used as the source IPv4 address for communication messages. If the Host Definition field was By Name, all IPv4 and IPv6 addresses will be displayed in this drop-down field. If the Host Definition field was By IP Address, only the existing IP addresses of the type specified in the IP Version field will be displayed.

  NOTE If the Auto option is selected, the system computes the source address based on the destination address.
- **Destination 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—**Enter the host address or name.
- **TTL—**Enter the maximum number of hops that Traceroute permits. This is used to prevent a case where the sent frame gets into an endless loop. The Traceroute command terminates when the destination is reached or when this value is reached. To use the default value (30), select **Use Default**.
- **Timeout—**Enter the length of time that the system waits for a frame to return before declaring it lost, or select **Use Default**.

STEP 3 Click **Activate Traceroute**. The operation is performed.

A page appears showing the Round Trip Time (RTT) and status for each trip in the fields:

- **Index—**Displays the number of the hop.
- **Host—**Displays a stop along the route to the destination.

- **Round Trip Time** *(1-3)*—Displays the round trip time in (ms) for the first through third frame and the status of the first through third operation.

6

Administration: Time Settings

Synchronized system clocks provide a frame of reference between all devices on the network. Network time synchronization is critical because every aspect of managing, securing, planning, and debugging a network involves determining when events occur. Without synchronized clocks, accurately correlating log files between devices when tracking security breaches or network usage is impossible.

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

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

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

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

- **System Time Options**
- **SNTP Modes**
- **Configuring System Time**

System Time Options

System time can be set manually by the user, dynamically from 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 device always configures the time, time zone, and DST. These parameters are obtained from the PC running the GUI, SNTP, values set manually, or if all else fails, from the factory defaults.

Time

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

- **Manual—**You must manually sets the time.
- **From PC—**Time can be received from the PC by using browser information.

  The configuration of time from the computer 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 the computer after reboot. The time after reboot is set during the first WEB login to the device.

  When you configure this feature for the first time, if the time was not already set, the device sets the time from the PC.

  This method of setting time works with both HTTP and HTTPS connections.

- **SNTP—**Time can be received from SNTP time servers. SNTP ensures accurate network time synchronization of the device up to the millisecond by using an SNTP server for the clock source. When specifying an SNTP server, if choosing to identify it by hostname, three suggestions are given in the GUI:
  - time-a.timefreq.bldrdoc.gov
  - time-b.timefreq.bldrdoc.gov
  - time-c.timefreq.bldrdoc.gov

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

NOTE SNTP is the recommended method for time setting.

Time Zone and Daylight Savings Time (DST)

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

- Dynamic configuration of the device 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 becomes the Operational time zone and DST, only if the dynamic configuration is disabled or fails.

  NOTE The DHCP server must supply DHCP option 100 in order for dynamic time zone configuration to take place.

SNTP Modes

The device can receive the system time from an SNTP server in one of the following ways:

- Client Broadcast Reception (passive mode)

  SNTP servers broadcast the time, and the device listens to these broadcasts. When the device is in this mode, there is no need to define a Unicast SNTP server.

- **Client Broadcast Transmission (active mode)**—The device, as an SNTP client, periodically requests SNTP time updates. This mode works in either of the following ways:
    - **SNTP Anycast Client Mode**—The device broadcasts time request packets to all SNTP servers in the subnet, and waits for a response.
    - **Unicast SNTP Server Mode**—The device sends Unicast queries to a list of manually-configured SNTP servers, and waits for a response.

The device supports having all of the above modes active at the same time and selects the best system time received from an SNTP server, according to an algorithm based on the closest stratum (distance from the reference clock).

Configuring System Time

Selecting Source of System Time

Use the System Time page to select the system time source. If the source is manual, you can enter the time here.

CAUTION If the system time is set manually and the device is rebooted, the manual time settings must be reentered.

To define system time:

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

The following fields are displayed:

- **Actual Time (Static)**—System time on the device. This shows the DHCP time zone or the acronym for the user-defined time zone if these were defined.
- **Last Synchronized Server**—Address, stratum and type of the SNTP server from which time was last taken.

STEP 2 Enter these parameters:

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

- **Main Clock Source (SNTP Servers)**—If you enable this, the system time is obtained from an SNTP server. To use this feature, you must also configure a connection to an SNTP server in the SNTP Interface Settings page. Optionally, enforce authentication of the SNTP sessions by using the SNTP Authentication page.
- **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 The Clock Source Setting needs to be set to either of the above in order for RIP MD5 authentication to work. This also helps features that associate with time, for example: Time Based ACL, Port, 802.1 port authentication that are supported on some devices.

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 the DHCP server 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 device*.

  NOTE The DHCP Client supports Option 100 providing dynamic time zone setting.

- **Time Zone from DHCP**—Displays the acronym of the time zone configured from the DHCP server. This acronym appears in the **Actual Time** field
- **Time Zone Offset**—Select the difference in hours between *Greenwich Mean Time* (GMT) and the local time. For example, the Time Zone Offset for Paris is GMT +1, while the Time Zone Offset for New York is GMT – 5.
- **Time Zone Acronym**—Enter a user-defined name that represents the time zone you have configured. This acronym appears in the **Actual Time** field.

Daylight Savings Settings—Select how DST is defined:

- Daylight Savings—Select to enable Daylight Saving Time.
- Time Set Offset—Enter the number of minutes offset from GMT ranging from 1—1440. The default is 60.
- Daylight Savings Type—Click one of the following:
  - *USA*—DST is set according to the dates used in the USA.
  - *European*—DST is set according to the dates used by the European Union and other countries that use this standard.
  - *By Dates*—DST is set manually, typically for a country other than the USA or a European country. Enter the following parameters:
  - *Recurring*—DST occurs on the same date every year.

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

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

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

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

Adding a Unicast SNTP Server

Up to 16 Unicast SNTP servers can be configured.

NOTE To specify a Unicast SNTP server by name, you must first configure DNS server(s) on the device (see **DNS Settings**). In order to add a Unicast SNTP server, check the box to enable **SNTP Client Unicast**.

To add a Unicast SNTP server:

STEP 1 Click **Administration** > **Time Settings** > **SNTP Unicast**.

STEP 2 Enter the following fields:

- **SNTP Client Unicast**—Select to enable the device to use SNTP-predefined Unicast clients with Unicast SNTP servers.

- **IPv4 Source Interface**—Select the IPv4 interface whose IPv4 address will be used as the source IPv4 address in messages used for communication with the SNTP server.
- **IPv6 Source Interface**—Select the IPv6 interface whose IPv6 address will be used as the source IPv6 address in messages used for communication with the SNTP server.

  NOTE If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

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

- **SNTP Server**—SNTP server IP address. 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 device.
- **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 values 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 device.
  - *In Process*—Occurs when the SNTP server has not fully trusted its own time server (i.e. when first booting up the SNTP 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.

- **Source**—How SNTP server was defined, for example: manually or from DHCPv6 server.
- **Interface**—Interface on which packets are received.

STEP 3 To add a Unicast SNTP server, enable **SNTP Client Unicast**.

STEP 4 Click Add.

STEP 5 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 select a well-known SNTP server by name from the list.

  NOTE To specify a well-known SNTP server, the device 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 **DNS Settings**)

- **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 NTP 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 NTP 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 device 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 6 Click **Apply**. The STNP server is added, and you are returned to the main page.

Configuring the SNTP Mode

The device can be in active and/or passive mode (see **SNTP Modes** for more information).

To enable receiving SNTP packets from all servers on the subnet and/or to enable transmitting time requests to SNTP servers:

STEP 1 Click **Administration** > **Time Settings** > **SNTP Multicast/Anycast**.

STEP 2 Select from the following options:

- **SNTP IPv4 Multicast Client Mode (Client Broadcast Reception)**—Select to receive system time IPv4 Multicast transmissions from any SNTP server on the subnet.
- **SNTP IPv6 Multicast Client Mode (Client Broadcast Reception)**—Select to receive system time IPv6 Multicast transmissions from any SNTP server on the subnet.
- **SNTP IPv4 Anycast Client Mode (Client Broadcast Transmission)**—Select to transmit SNTP IPv4 synchronization packets requesting system time information. The packets are transmitted to all SNTP servers on the subnet.
- **SNTP IPv6 Anycast Client Mode (Client Broadcast Transmission)**—Select to transmit SNTP IPv6 synchronization packets requesting system time information. The packets are transmitted to all SNTP servers on the subnet.

STEP 3 If the system is in Layer 3 system mode, click **Add** to select the interface for SNTP reception/transmission.

Select an interface and select the reception/transmission options.

STEP 4 Click **Apply** to save the settings to the Running Configuration file.

Defining SNTP Authentication

SNTP clients can authenticate responses by using HMAC-MD5. An SNTP server is associated with a key, which is used as input together with the response itself to the MD5 function; the result of the MD5 is also included in the response packet.

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 information.

Workflow

STEP 1 Enable authentication in the SNTP Authentication page.

STEP 2 Create a key in the SNTP Authentication page.

STEP 3 Associate this key with an SNTP server in the SNTP Unicast page.

To enable SNTP authentication and define keys:

STEP 1 Click **Administration** > **Time Settings** > **SNTP Authentication**.

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

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

STEP 4 Click **Add.**

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 device to synchronize to it.
- **Trusted Key**—Select to enable the device to receive synchronization information only from a SNTP server by using this authentication key.

STEP 6 Click **Apply**. The SNTP Authentication parameters are written to the Running Configuration file.

Time Range

Time ranges can be defined and associated with the following types of commands, so that they are applied only during that time range:

- ACLs
- 8021X Port Authentication
- Port Stat
- Time-Based PoE

There are two types of time ranges:

- **Absolute** —This type of time range begins on a specific date or immediately and ends on a specific date or extends infinitely. It is created in the Time Range pages. A recurring element can be added to it.
- **Recurring** — This type of time range contains a time range element that is added to an absolute range, and begins and ends on a recurring basis. It is defined in the Recurring Range pages.

If a time range includes both absolute and recurring ranges, the process associated with it is activated only if both absolute start time and the recurring time range have been reached. The process is deactivated when either of the time ranges is reached.

The device supports a maximum of 10 absolute time ranges.

All time specifications are interpreted as local time (Daylight Saving Time does not affect this).To ensure that the time range entries take effect at the desired times, the system time must be set.

The time-range feature can be used for the following:

- Limit access of computers to the network during business hours (for example), after which the network ports are locked, and access to the rest of the network is blocked (see **Chapter 9, "Configuring Ports"** and **Chapter 9, "Configuring LAG Settings"**)

- Limit PoE operation to a specified period.

Absolute Time Range

To define an absolute time range:

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

The existing time ranges are displayed.

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

STEP 3 Enter the following fields:

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

STEP 4 To add a recurring time range, click **Recurring Range**.

Recurring Time Range

A recurring time element can be added to an absolute time range. This limits the operation to certain time periods within the absolute range.

To add a recurring time range element to an absolute time range:

STEP 1 Click **Administration** > **Time Settings** > **Recurring Range**.

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

STEP 2 Select the absolute time range to which to add the recurring range.

STEP 3 To add a new recurring time range, click **Add**.

STEP 4 Enter the following fields:

- **Recurring Starting Time—**Enter the date and time that the Time Range begins on a recurring basis.

Recurring Ending Time—Enter the date and time that the Time Range ends on a recurring basis.

7

Administration: Diagnostics

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

It covers 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 Test 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 when testing cables using (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**.

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

STEP 3 Click **Copper Test**.

STEP 4 When the message appears, click **OK** to confirm that the link can go down or **Cancel** to abort the test.

The following fields are displayed in the Test Results block:

- **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 contains the following information, which is refreshed each time you enter the page:

- **Cable Length:** Provides an estimate for the length.
- **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

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**.

This page displays the following fields:

- **Port—**Port number on which the SFP is connected.
- **Description—**Description of optical transceiver.
- **Serial Number—**Serial number of optical transceiver.
- **PID—**VLAN ID.
- **VID—**ID of optical transceiver.
- **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 device to send a copy of network packets seen on one device port, multiple device ports, or an entire VLAN to a network monitoring connection on another port on the device. 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 device 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.

VLAN mirroring is not active on a VLAN that was not manually created. For example, if VLAN 23 was created by GVRP, and you manually created VLAN 34, and you create port mirroring that includes VLAN 23, VLAN 34, or both, and later on delete VLAN 34, the status in port mirroring is set to **Not Ready**, because the VLAN34 is no longer in the database and VLAN23 was not created manually.

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 following fields are displayed:

- **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 (Rx), outgoing from the port (Tx), 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.

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 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 to the Running Configuration.

Viewing CPU Utilization and Secure Core Technology

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

The device 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 device operation. The device uses the Secure Core Technology (SCT) feature to ensure that the device receives and processes 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**.

The CPU Utilization page appears.

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

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

STEP 2 Select the **Refresh Rate** (time period in seconds) that passes before the statistics are refreshed. A new sample is created for each time period

8

Administration: Discovery

This section provides information for configuring Discovery.

It covers the following topics:

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

Bonjour

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

Bonjour in Layer 2 System Mode

When the device is in Layer 2 system mode, Bonjour Discovery is enabled globally; it cannot be enabled on a per-port or per-VLAN basis. The device advertises all of the services that have been turned on by the administrator based on the configuration on the Services page.

When Bonjour Discovery and IGMP are both enabled, the IP Multicast address of Bonjour appears on the Adding IP Multicast Group Address page.

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

To globally enable Bonjour when the system is in Layer 2 system mode:

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

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

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

Bonjour in Layer 3 System Mode

In Layer 3 system mode, each interface (VLAN, port, or LAG) can be assigned an IP address. When Bonjour is enabled, the device can send Bonjour Discovery packets on all interfaces that have IP addresses. Bonjour can individually be assigned on a per-port and/or per-VLAN basis. When Bonjour is enabled, the device can send Bonjour Discovery packets to interfaces with IP addresses that have been associated with Bonjour on the Bonjour Discovery Interface Control table. (When the device is operating in Layer 3 system mode, go to **IP Configuration** > **Management and IP Interface** > **IPv4 Interface** to configure an IP address to an interface.)

If an interface, such as a VLAN, is deleted, Goodbye packets are sent to deregister services the device is advertising from the neighboring cache table within the local network. The Bonjour Discovery Interface Control Table shows interfaces with IP addresses that are associated with the Bonjour feature. Any Bonjour advertisement can only be broadcasted to interfaces listed in this table. (See the Bonjour Discovery Interface Control Table on the Administration > Discovery - Bonjour page. If the available services are changed, those changes are advertised, deregistering services that are turned off and registering services that are turned on. If an IP address is changed, that change is advertised.

If Bonjour is disabled, the device does not send Bonjour Discovery advertisements and it does not listen for Bonjour Discovery advertisements sent by other devices.

To configure Bonjour when the device is in Layer 3 system mode:

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

STEP 2 Select **Enable** to enable Bonjour discovery globally.

STEP 3 Click **Apply** to update the Running Configuration file.

STEP 4 To enable Bonjour on an interface, click **Add.**

STEP 5 Select the interface, and click **Apply**.

NOTE Click **Delete** to disable Bonjour on an interface (this performs the delete operation without any additional operation, such as Apply).

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 device 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 CDP/LLDP configuration notes apply:

- 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 device filters out incoming CDP/LLDP packets from ports that are CDP/LLDP-disabled.
- If CDP/LLDP is globally disabled, the device 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 device is enabled to send out CDP and LLDP advertisement based on the voice VLAN configured at the device. 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 device transmits and receives 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 according to 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. 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 covers the following topics:

- **LLDP Overview**
- **Setting LLDP Properties**
- **Editing LLDP Port Settings**
- **LLDP MED Network Policy**
- **Configuring LLDP MED Port Settings**
- **Displaying LLDP Port Status**

- **Displaying LLDP Local Information**
- **Displaying LLDP Neighbors Information**
- **Accessing LLDP Statistics**
- **LLDP Overloading**

LLDP Overview

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 device 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 Network Policy**.

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 device'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, such as enabling/disabling the feature globally and setting timers.

To enter LLDP properties:

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

STEP 2 Enter the parameters.

- **LLDP Status**—Select to enable LLDP on the device (enabled by default).
- **LLDP Frames Handling**—If LLDP 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 SNMP Notification Interval**—Enter the minimum time interval between SNMP 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.

- **Chassis ID Advertisement**—Select one of the following options for advertisement in the LLDP messages:
    - *MAC Address*—Advertise the MAC address of the device.
    - *Host Name*—Advertise the host name of the device.

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

STEP 4 Click **Apply**. The LLDP properties are added to the Running Configuration file.

Editing LLDP Port Settings

The Port Settings page enables activating LLDP and SNMP notification per port, and entering the TLVs that are sent in the LLDP PDU.

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

To define the LLDP port settings:

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

This page contains the port LLDP information.

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

This page provides the following fields:

- **Interface**—Select the port to edit.
- **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.

- **SNMP Notification**—Select **Enable** to send notifications to SNMP notification recipients; for example, an SNMP managing system, when there is a topology change.

  The time interval between notifications is entered in the Topology Change SNMP Notification Interval field in the LLDP Properties page. Define SNMP Notification Recipients by using the SNMP > Notification Recipient v1,2 and/or SNMP > Notification Recipient v3 page.

- **Available Optional TLVs**—Select the information to be published by the device 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 device. The value equals the sysDescr object.
  - *System Capabilities*—Primary functions of the device, and whether or not these functions are enabled in 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.
  - *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 device:

    - *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. We recommend you select this option when the device is in Layer 3 system mode and the device is configured with multiple IP addresses (this is always true on SG500X/ESW2-550X devices).
- **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 written to the Running Configuration file.

LLDP MED Network Policy

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

- Enables the advertisement and discovery of network polices 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, can be included in the outgoing LLDP packets to the attached LLDP media endpoint device. The media endpoint device must send its traffic as specified in the network policy it receives. For example, a policy can be created for VoIP traffic that instructs VoIP phone to:

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

Network policies are associated with ports by using the LLDP MED Port Settings 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 device to automatically generate and advertise a network policy for voice application based on the voice VLAN maintained by the device. Refer the Auto Voice VLAN section for details on how the device maintains its voice VLAN.

To define an LLDP MED network policy:

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

This page contains previously-created network policies.

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

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

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

STEP 4 To define a new policy, click **Add**.

STEP 5 Enter the values:

- **Network Policy Number—**Select the number of the policy to be created.
- **Application—**Select the type of application (type of traffic) for which the network policy is being defined.
- **VLAN ID—**Enter the VLAN ID to which the traffic must be sent.

- **VLAN Tag**—Select whether the traffic is Tagged or Untagged.
- **User Priority**—Select the traffic priority applied to traffic defined by this network policy. This is the CoS value.
- **DSCP Value**—Select the DSCP value to associate with application data sent by neighbors. This informs them how they must mark the application traffic they send to the device.

STEP 6 Click **Apply**. The network policy is defined.

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

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 device automatically generates 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**.

This page contains 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.**

STEP 4 Enter the parameters:

- **Interface**—Select the interface to configure.
- **LLDP MED Status**—Enable/disable LLDP MED on this port.

- **SNMP Notification—**Select whether SNMP notification is sent on a per-port basis when an end station that supports MED is discovered; for example a SNMP managing system, when there is a topology change.
- **Available Optional TLVs—**Select the TLVs that can be published by the device by moving them to the *Selected Optional TLVs* list.
- **Available Network Policies—**Select the LLDP MED policies to 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 written to the Running Configuration file.

Displaying LLDP Port Status

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

STEP 1 To view the LLDP port status, click **Administration** > **Discovery - LLDP** > **LLDP Port Status**.

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

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

LLDP Port Status Global Information

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

LLDP Port Status Table

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

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

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

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

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

This page displays the following fields:

Global

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

Management Address

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

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

MAC/PHY Details

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

802.3 Details

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

802.3 Link Aggregation

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

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, 911, Layer 2 device 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 contains information that was received from neighboring devices.

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

To view the LLDP neighbors information:

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

This page contains 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 device.
- **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 LLDP Neighbor Information page contains 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)

- **Remote 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).

- **Remote 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).
- **Local Tx Echo**—Indicates the local link partner's reflection of the remote link partner's Tx value.
- **Local 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 Table

- **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**.

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**.

This page contains 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**.

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

- **LLDP Mandatory TLVs**
    - *Size (Bytes)*—Total mandatory TLV byte size.
    - *Status*—If the mandatory TLV group is being transmitted, or if the TLV group was overloaded.
- **LLDP MED Capabilities**
    - *Size (Bytes)*—Total LLDP MED capabilities packets byte size.
    - *Status*—If the LLDP MED capabilities packets 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 covers the following topics:

- **Setting CDP Properties**
- **Editing CDP Interface Settings**
- **Displaying CDP Local Information**
- **Displaying CDP Neighbors Information**
- **Viewing CDP Statistics**

Setting CDP Properties

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 followings is sample workflow in configuring CDP on the device. You can also find additional CDP configuration guidelines in the LLDP/CDP section.

STEP 1 Enter the CDP global parameters using the CDP Properties page

STEP 2 Configure CDP per interface using the Interface Setting page

STEP 3 If Auto Smartport is to detect the capabilities of CDP devices, enable CDP in the Smartport Properties page.

See **Identifying Smartport Type** for a description of how CDP is used to identify devices for the Smartport feature.

To enter CDP general parameters:

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

STEP 2 Enter the parameters.

- **CDP Status**—Select to enable CDP on the device.
- **CDP Frames Handling**—If CDP is not enabled, select the action to be taken if a packet that matches the selected criteria is received:
  - *Bridging*—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 device 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). The following options are possible:
    - *MAC Address*—Use the MAC address of the device as the device ID.
    - *Serial Number*—Use the serial number of the device as the device ID.
    - *Host Name*—Use the host name of the device as the device ID.
- **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

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

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 CDP interface settings:

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

This page contains 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 (Voice VLAN/ Native VLAN/Duplex).
- **No. of Neighbors**—Number of neighbors detected.

The bottom of the page has four buttons:

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

This page provides the following fields:

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

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

- **Syslog Voice VLAN Mismatch—**Select to enable 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 written to the Running Configuration.

Displaying CDP Local Information

To view information that is advertised by the CDP protocol about the local device:

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

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 TLV**
  - **Device ID Type—**Type of the device ID advertised in the device ID TLV.
  - **Device ID—**Device ID advertised in the device ID TLV.

- System Name TLV
  - **System Name—**System name of the device.
- Address TLV
  - **Address1-3—**IP addresses (advertised in the device address TLV).
- Port TLV
  - **Port ID**—Identifier of port advertised in the port TLV.
- Capabilities TLV
  - **Capabilities**—Capabilities advertised in the port TLV)
- Version TLV
  - **Version**—Information about the software release on which the device is running.
- Platform TLV
  - **Platform**—Identifier of platform advertised in the platform TLV.
- Native VLAN TLV
  - **Native VLAN**—The native VLAN identifier advertised in the native VLAN TLV.
- Full/Half Duplex TLV
  - **Duplex**—Whether port is half or full duplex advertised in the full/half duplex TLV.
- Appliance TLV
  - **Appliance ID**—Type of device attached to port advertised in the appliance TLV.
  - **Appliance VLAN ID—**VLAN on the device used by the appliance, for instance if the appliance is an IP phone, this is the voice VLAN.
- Extended Trust TLV
  - **Extended Trust—**Enabled indicates that the port is trusted, 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 TLV
    - **CoS for Untrusted Ports**—If Extended Trust is disabled on the port, this fields displays the Layer 2 CoS value, meaning, an 802.1D/802.1p priority value. This is the COS value with which all packets received on an untrusted port are remarked by the device.
- Power TLV
    - **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 **Neighbor Information**.

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

- **Device ID**—Neighbors device ID.

- **System Name**—Neighbors system name.
- **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**.

This page contains the following fields about the neighbor:

- **Device ID**—Identifier of the neighboring device ID.
- **System Name**—Name 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 neighbors platform.
- Neighbor Interface—Interface number of the neighbor through which frame arrived.
- Native VLAN—Neighbors native VLAN.
- Duplex—Whether neighbors interface is half or full duplex.
- Addresses—Neighbors addresses.
- Power Drawn—Amount of power consumed by neighbor on the interface.
- Version—Neighbors software version.

NOTE Clicking on the **Clear Table** button disconnect all connected devices if from CDP, and if Auto Smartport is enabled 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 following fields are displayed for every interface:.

Packets Received/Transmitted:

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

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 all counters on all interfaces, click **Clear All Interface Counters**. To clear all counters on an interface, select it and click **Clear All Interface Counters**.

Port Management

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

It covers the following topics:

- **Configuring Ports**
- **Setting Port Configuration**
- **Link Aggregation**
- **UDLD**
- **Configuring Green Ethernet**

Configuring Ports

To configure ports, perform the following actions:

1. Configure port by using the Port Settings 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 device, configure the device as described in **Port Management: PoE**.

Setting Port Configuration

Ports can be configured in the following pages.

Port Settings

The Port Settings 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 Settings page.

To configure port settings:

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

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 2,000 bytes. For jumbo frames to take effect, the device must 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 device is rebooted.

STEP 4 To update the port settings, select the desired port, and click **Edit.**

STEP 5 Modify the following parameters:

- **Port**—Select the port number.
- **Port Description**—Enter the port user-defined name or comment.
- **Port Type**—Displays the port type 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).
  - 10G-Fiber Optics—Ports with speed of either 1G or 10G.

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

- **Administrative Status**—Select whether the port must be Up or Down when the device is rebooted.
- **Operational Status**—Displays whether the port is currently Up or Down. If the port is down because of an error, the description of the error is displayed.
- **Link Status SNMP Traps**—Select to enable generation of SNMP traps that notify of changes to the link status of the port.
- **Time Range**—Select to enable the time range during which the port is in Up state. When the time range is not active, the port is in shutdown. If a time range is configured, it is effective only when the port is administratively Up. If a time range is not yet defined, click **Edit** to go to the Time Range page.
- **Time Range Name**—Select the profile that specifies the time range.
- **Operational Time-Range State**—Displays whether the time range is currently active or inactive.
- **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, STP loopback guard or Access Control List (ACL) configurations. 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.
- **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 device and the client in both directions simultaneously.
  - *Half*—The interface supports transmission between the device and the client in only one direction at a time.
- **Operational Duplex Mode—**Displays the ports 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 ports 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 device 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 device to a station by using a straight through cable.
  - *Auto*—Select to configure this device to automatically detect the correct pinouts for the connection to another device.

- **Operational MDI/MDIX**—Displays the current MDI/MDIX setting.
- **Protected Port**—Select to make this a protected port. (A protected port is also referred as a Private VLAN Edge (PVE).) The features of a protected port are as follows:
  - Protected Ports provide Layer 2 isolation between interfaces (Ethernet ports and LAGs) that share the same VLAN.
  - Packets received from protected ports can be forwarded only to unprotected egress ports. Protected port filtering rules are also applied to packets that are forwarded by software, such as snooping applications.
  - Port protection is not subject to VLAN membership. Devices connected to protected ports are not allowed to communicate with each other, even if they are members of the same VLAN.
  - Both ports and LAGs can be defined as protected or unprotected. Protected LAGs are described in the **Configuring LAG Settings** section.
- **Member in LAG**—If the port is a member of a LAG, the LAG number appears; otherwise this field is left blank.

STEP 6 Click **Apply**. The Port Settings are written to the Running Configuration file.

Error Recovery Settings

This page enables automatically reactivating a port that has been shutdown because of an error condition.

To configure error recovery settings:

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

STEP 2 Enter the following fields:

- **Automatic Recovery Interval**—Select to enable the error recovery mechanism for the port security err-disable state.

- **Port Security**—Select to enable the error recovery mechanism for the port security err-disable state.
- **802.1x Single Host Violation**—Select to enable error recovery mechanism for the 802.1x error-disable state.
- **ACL Deny**—Select to enable. error recovery mechanism for the ACL deny error-disable state.
- **STP BPDU Guard**—Select to enable the error recovery mechanism for thee STP BPDU guard error-disable state.
- **UDLD**—Select to enable error recovery mechanism for the UDLD shutdown state.

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

To manually reactivate a port:

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

The list of inactivated interfaces along with their **Suspension Reason** is displayed.

STEP 2 Select the interface to be reactivated.

STEP 3 Click **Reactivate**.

Link Aggregation

This section describes how to configure LAGs. It covers 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 enables 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 to applying), then the LACP button 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

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 Layer 2 or Layer 3 packet header information.

The device 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

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 device supports 32 LAGs with up to 8 ports in a LAG group.

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.

Default Settings and Configuration

Ports are not members of a LAG and are not candidates to become part of a LAG.

Static and Dynamic LAG Workflow

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 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. Enable LACP on the LAG. Assign up to 16 candidates ports to the dynamic LAG by selecting and moving the ports from the **Port List** to the **LAG Members** List 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.**

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 saved to the Running Configuration file.

To define the member or candidate ports in a LAG.

STEP 1 Select the LAG to be configured, and click **Edit.**

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**. LAG membership is saved to the Running Configuration file.

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**.

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

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.
- **Link Status SNMP Traps—**Select to enable generation of SNMP traps notifying of changes to the link status of the ports in the LAG.
- **Time Range—**Select to enable the time range during which the port is in Up state. When the time range is not active, the port is in shutdown. If a time range is configured, it is effective only when the port is administratively Up. If a time range is not yet defined, click **Edit** to go to the Time Range page.
- **Time Range Name—**Select the profile that specifies the time range.
- **Operational Time-Range State—**Displays whether the time range is currently active or inactive.
- **Reactivate Suspended LAG—**Select to reactivate a port if the LAG has been disabled through the locked port security option or through ACL configurations.

- **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.
- **Administrative Flow Control—**Set Flow Control to either **Enable** or **Disable** or enable the **Auto-Negotiation** of Flow Control on the LAG.
- **Operational Flow Control—**Displays the current Flow Control setting.
- **Protected LAG—**Select to make the LAG a protected port for Layer 2 isolation. See the Port Configuration description in **Setting Basic Port Configuration** for details regarding protected ports and LAGs.

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 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 device on the controlling end of the link uses port priorities to determine which ports are bundled into the LAG and which ports are put in hot-standby mode. Port priorities on the other device (the non-controlling end of the link) are ignored.

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

- Any link operating at a different speed from the highest-speed active member or operating at half-duplex 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.

LACP With No Link Partner

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

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

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

Setting LACP Parameter Settings

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

With all factors equal, when the LAG is configured with more candidate ports than the maximum number of active ports allowed (8), the device selects ports as active from the dynamic LAG on the device that has the highest priority.

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

To define the LACP settings:

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

STEP 2 Enter the LACP System Priority. See **LACP Priority and Rules**.

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

STEP 4 Enter the values for the following fields:

- **Port—**Select the port number to which timeout and priority values are assigned.
- **LACP Port Priority—**Enter the LACP priority value for the port. See **Setting LACP Parameter Settings**.
- **LACP Timeout—**Time interval between the sending and receiving of consecutive LACP PDUs. Select the periodic transmissions of LACP PDUs, which occur at either a **Long** or **Short** transmission speed, depending upon the expressed LACP timeout preference.

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

UDLD

See **Port Management: Unidirectional Link Detection**.

PoE

See **Port Management: PoE**.

Configuring Green Ethernet

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

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 device 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 **802.3az Energy Efficient Ethernet Feature** 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 be disabled. If Short Reach Mode is enabled, EEE be grayed out.

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

The device LEDs are power consumers. Since most of the time the devices are in an unoccupied room, having these LEDs lit is a waste of energy. The Green Ethernet feature enables you to disable the port LEDs (for link, speed, and PoE) when they are not required, and to enable the LEDs if they are needed (debugging, connecting additional devices etc.).

On the System Summary page, the LEDs that are displayed on the device board pictures are not affected by disabling the LEDs.

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

The saved energy displayed is only related to Green Ethernet. The amount of energy saved by EEE is not displayed.

Power Saving by Disabling Port LEDs

The Disable Port LEDs feature allows the user to save extra power consumed by device LEDs. Since most of the time the devices are in an unoccupied room, having these LEDs lit is a waste of energy. The Green Ethernet feature enables you to disable the port LEDs (for link, speed, and PoE) when they are not required, and to enable the LEDs if they are needed (debugging, connecting additional devices etc.).

On the System Summary page, the LEDs that are displayed on the device board pictures are not affected by disabling the LEDs.

On the Green Ethernet -> Properties page, the device enables the user to disable the ports LEDs in order to save power.

802.3az Energy Efficient Ethernet Feature

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

It covers 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 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 (device 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 to 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 still e 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 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 Setting page.

b. Select **Auto Negotiation** field to ensure that it is Enabled.

STEP 2 Ensure that **802.3 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 Setting page.

b. Check the **802.3 Energy Efficient 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 Energy Efficient Ethernet (EEE) LLDP** (it is enabled by default).

STEP 4 To see 802.3 EEE-related information on the local device, open the Administration > Discovery LLDP >LLDP Local Information page, and view the information in the 802.3 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 device. 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**.

STEP 2 Enter the values for the following fields:

- **Energy Detect Mode—**Disabled by default. Click the checkbox to enable.
- **Short Reach—**Globally enable or disable Short Reach mode if there are GE ports on the device.

  NOTE If Short Reach is enabled, EEE must be disabled.
- **Port LEDs—**Select to enable the port LEDs. When these are disabled, they do not display link status, activity, etc.
- **Power Savings—**Displays the percentage of power saved by running Green Ethernet and Short Reach. The power savings displayed is only relevant to the power saved by Short Reach and Energy Detect modes. The EEE power savings is dynamic by nature since it is based on port utilization and is therefore not taken into consideration. The power saving calculation is performed by comparing the maximum power consumption without power savings to the current consumption.
- **Cumulative Energy Saved—**Displays the amount of energy saved from the last device reboot. This value is updated each time there is an event that affects power saving.
- **802.3 Energy Efficient Ethernet (EEE)—** Globally enable or disable EEE mode.

STEP 3 Click **Apply**. The Green Ethernet Properties are written to the Running Configuration file.

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 displays the following:

- **Global Parameter Status—**Describes the enabled features.

For each port the following fields are described:

- **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 **Setting Global Green Ethernet Properties**.

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

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 written to the Running Configuration file.

10

Port Management: Unidirectional Link Detection

This section describes how the Unidirectional Link Detection (UDLD) feature.

It covers the following topics:

- **UDLD Overview**
- **UDLD Operation**
- **Usage Guidelines**
- **Dependencies On Other Features**
- **Default Settings and Configuration**
- **Before You Start**
- **Common UDLD Tasks**
- **Configuring UDLD**

UDLD Overview

UDLD is a Layer 2-protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to detect unidirectional links. A unidirectional link occurs whenever traffic from a neighboring device is received by the local device, but traffic from the local device is not received by the neighbor.

The purpose of UDLD is to detect ports on which the neighbor does not receive traffic from the local device (unidirectional link) and to shut down those ports.

All connected devices must support UDLD for the protocol to successfully detect unidirectional links. If only the local device supports UDLD, it is not possible for the device to detect the status of the link. In this case, the status of the link is set to undetermined. The user can configure whether ports in the undetermined state are shut down or merely trigger notifications.

UDLD Operation

UDLD States and Modes

Under the UDLD protocol, ports are assigned the following states:

- **Detection—**System is attempting to determine whether the link is bidirectional or unidirectional. This is a temporary state.
- **Bidirectional—**Traffic sent by a local device is known to be received by its neighbor, and traffic from the neighbor is received by the local device.
- **Shutdown—**The link is unidirectional. Traffic sent by a local device is received by its neighbor, but traffic from the neighbor is not received by the local device.
- **Undetermined—**The system cannot determine the state of the port, because of one of the following is occurring:
    - The neighbor does not support UDLD.

      or
    - The neighbor does not receive traffic from the local device.

  The UDLD action in this case depends on the UDLD mode of the device as explained below.

UDLD supports the following modes of operation:

- **Normal**
    - If the link is unidirectional, the port is shut down.
    - If the link is undetermined, the port is not shut down. Its status is changed to undetermined and a notification is sent.
- **Aggressive**

  If the link is unidirectional or undetermined, the port is shut down.

UDLD is enabled on a port when one of the following occurs:

- The port is a fiber port and UDLD is enabled globally.
- The port is a copper port and you specifically enable UDLD on it.

How UDLD Works

When UDLD is enabled on a port, the following actions are performed:

- UDLD initiates the detection state on the port.

  In this state, UDLD periodically sends messages on every active interface to all neighbors. These messages contain the device ID of all known neighbors. It sends these messages according to a user-defined message time.

- UDLD receives UDLD messages from neighboring devices. It caches these messages until the expiration time (3 times message time) has passed. If a new message is received before the expiration time, the information in that message replaces the previous one.

- When the expiration time expires, the device does the following with the information received:

  - **If the neighbor message contains the local device ID**—The link status of the port is set to bidirectional.
  - **If the neighbor message does not contain the local device ID**—The link status of the port is set to unidirectional, and the port is shut down.

- If UDLD messages are not received from a neighboring device during the expiration time frame, the link status of the port is sent to undetermined and the following occurs:

  - **Device is in normal UDLD mode:** A notification is issued.
  - **Device is in aggressive UDLD mode.** The port is shut down.

While the interface is in the bidirectional or the undetermined state, the device periodically sends a message each message time seconds. The above steps are performed over and over.

A port that was shut down can be reactivated manually in the Port Management > Error Recovery Settings page. For more information, see **Reactivating a Shutdown Port**.

If an interface is down and UDLD is enabled, the device removes all neighbor information and sends at least one ULDL message to the neighbors informing them that the port is down. When the port is brought up, the UDLD state is changed to detection.

UDLD Not Supported or is Disabled on a Neighbor

If UDLD is not supported or disabled on a neighbor, then no UDLD messages are received from that neighbor. In this case, the device cannot determine whether the link is unidirectional or bidirectional. The status of the interface is then set to undetermined. The actions taken by the device depend on whether the UDLD mode is normal or aggressive.

Inconsistent UDLD Mode in Local and Neighboring Device

It is possible for the local device and its neighbor to be set to a different UDLD mode (normal, aggressive). The UDLD mode is not contained in the UDLD messages, so that the local device does not know the UDLD mode of the neighbor and vice versa.

If the UDLD modes are different on the local and neighbor device, the devices act as follows:

- When the UDLD state of the link is bidirectional or unidirectional, both devices shut down their ports.
- When the UDLD state of the port is undetermined, the side with the normal UDLD mode merely issues a notification, while the side with the aggressive UDLD mode shuts down the port.

If both devices are in normal mode, the port is not shut down when its state is undetermined.

Reactivating a Shutdown Port

You can reactivate a port that was shut down by UDLD in one of the following ways:

- **Automatically**—You can configure the system to automatically reactivate ports shut down by UDLD in the Port Management > Error Recovery Settings page. In this case, when a port is shut down by UDLD, it is automatically reactivated when the automatic recovery interval expires.

UDLD again begins running on the port. If the link is still unidirectional, UDLD shuts it down again after the UDLD expiration time expires, for instance.

- **Manually—**You can reactivate a port in the Port Management > Error Recovery Settings page

Usage Guidelines

Cisco does not recommend enabling UDLD on ports that are connected to devices on which UDLD is not supported or disabled. Sending UDLD packets on a port connected to a device that does not support UDLD simply causes more traffic on the port without providing benefits.

In addition, take the following into consideration when configuring UDLD:

- Set the message time according to how urgent it is to shut down ports with a unidirectional link. The lower the message time, the more UDLD packets are sent and analyzed, but the sooner the port is shut down if the link is unidirectional.
- If you want UDLD to be enabled on a copper port, you must enable it per port. When you globally enable UDLD, it is only enabled on fiber ports.
- Set the UDLD mode to normal when you do not want to shut down ports unless it is known for sure that the link is unidirectional.
- Set the UDLD mode to aggressive when you want to shut down any port whenever there is even a chance that the link is undetermined.

Dependencies On Other Features

- UDLD and Layer 1.

  When UDLD is enabled on a port, UDLD actively runs on that port while the port is up. When the port is down, UDLD goes into UDLD shutdown state. In this state, UDLD removes all learned neighbors. When the port is changed from down to up, UDLD resumes actively running.

- UDLD and Layer 2 Protocols

  UDLD runs on a port independently from other Layer 2 protocols running on the same port, such as STP or LACP. For example, UDLD assigns the port a status regardless of the STP status of the port or regardless of whether the port belongs to a LAG or not.

Default Settings and Configuration

The following defaults exist for this feature:

- UDLD is disabled by default on all ports of the device.
- Default message time is 15 seconds.
- Default expiration time is 45 seconds (3 times the message time).
- Default port UDLD state:
  - Fiber interfaces are in the global UDLD state.
  - Non-fiber interfaces are in the disable state.

Before You Start

No preliminary tasks are required.

Common UDLD Tasks

This section describes some common tasks to setup UDLD.

Workflow1: *To globally enable UDLD on fiber ports, perform the following steps:*

STEP 1 Open the Port Management > UDLD Global Settings page.

a. Enter the **Message Time**.

b. Select either **Disabled**, **Normal** or **Aggressive** as the global UDLD status.

STEP 2 Click Apply

Workflow2: To change the UDLD configuration of a fiber port or to enable UDLD on a copper port, perform the following steps:

STEP 1 Open the **Port Management > UDLD Global Settings** page.

a. Select a port.

b. Select either **Default**, **Disabled**, **Normal** or **Aggressive** as the port's UDLD status. If you select Default, the port receives the global setting.

STEP 2 Click Apply.

Workflow3: To bring a port up after it was shut down by UDLD and automatic reactivation was not configured:

STEP 1 Open the **Port Management** > **Error Recovery Settings** page.

a. Select a port.

b. Click Reactivate.

Configuring UDLD

The UDLD feature can be configured for all fiber ports at one time (in the UDLD Global Settings page) or per port (in the UDLD Interface Settings page).

UDLD Global Settings

The Fiber Port UDLD Default State is only applicable to fiber ports.

The Message Time field is applicable to both copper and fiber ports.

To configure UDLD globally:

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

STEP 2 Enter the following fields:

- **Message Time**—Enter the interval between two sent UDLD messages. This field is relevant for both fiber and copper ports.

- **Fiber Port UDLD Default State—**This field is only relevant for **fiber** ports. The UDLD state of copper ports must be set individually in the UDLD Interface Settings page. The possible states are:
  - *Disabled*—UDLD is disabled on all ports of the device.
  - *Normal*—Device shuts down an interface if the link is unidirectional. If the link is undetermined, a notification is issued.
  - *Aggressive*—Device shuts down an interface if the link is unidirectional or undetermined.

STEP 3 Click **Apply** to save the settings to the Running Configuration file.

UDLD Interface Settings

Use the UDLD Interface Settings page to change the UDLD state for a specific port. Here the state can be set for copper or fiber ports.

To copy a particular set of values to more than one port, set that value for one port and use the **Copy** button to copy it to the other ports.

To configure UDLD for an interface:

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

Information is displayed for all ports on which UDLD is enabled, or, if you have filtered only a certain group of ports, information is displayed for that group of ports.

- **Port—**The port identifier.
- **UDLD State—**The possible states are:
  - *Disabled*—UDLD is disabled on all fiber ports of the device.
  - *Normal*—Device shuts down an interface if it detects that the link is unidirectional. It issues a notification if the link is undetermined.
  - *Aggressive*—Device shuts down a port if the link is unidirectional or undetermined.
- **Bidirectional State—**Select the value of this field for the selected port. The possible states are:
  - *Detection*—The latest UDLD state of the port is in the process of being determined. Expiration time has not yet expired since the last

determination (if there was one), or since UDLD began running on the port, so that the state is not yet determined.

  - *Bidirectional*—Traffic sent by the local device is received by its neighbor, and traffic from the neighbor is received by the local device.
  - *Undetermined*—The state of the link between the port and its connected port cannot be determined either because no UDLD message was received or the UDLD message did not contain the local device ID in it.
  - *Disabled*—UDLD has been disabled on this port.
  - *Shutdown*—The port has been shut down because its link with the connected device is unidirectional or undetermined in aggressive mode.

- **Number of Neighbors**—Number of connected devices detected.

STEP 2 To modify the UDLD state for a specific port, select it and click **Edit**.

STEP 3 Modify the value of the UDLD state. If you select **Default**, the port receives the value of the **Fiber Port UDLD Default State** in the Global UDLD Settings page.

STEP 4 Click **Apply** to save the settings to the Running Configuration file.

UDLD Neighbors

To view all devices connected to the local device:

STEP 1 Click **Port Management > UDLD** > **UDLD Neighbors**.

The following fields are displayed for all UDLD-enabled ports.

- **Interface Name**—Name of the local UDLD-enabled port.
- **Neighbor Information:**
  - *Device ID*—ID of the remote device.
  - *Device MAC*—MAC address of the remote device.
  - *Device Name*—Name of the remote device.
  - *Port ID*—Name of the remote port.

- **State**—State of the link between the local and neighboring device on the local port. The following values are possible:
  - *Detection*—The latest UDLD state of the port is in the process of being determined. Expiration time has not yet expired since the last determination (if there was one), or since UDLD began running on the port, so that the state is not yet determined.
  - *Bidirectional*—Traffic sent by the local device is received by its neighbor, and traffic from the neighbor is received by the local device.
  - *Undetermined*—The state of the link between the port and its connected port cannot be determined either because no UDLD message was received or the UDLD message did not contain the local device ID in it.
  - *Disabled*—UDLD has been disabled on this port.
  - *Shutdown*—The port has been shut down because its link with the connected device is unidirectional or undetermined in aggressive mode.
- **Neighbor Expiration Time (Sec)**—Displays the time that must pass before determining the port UDLD status. This is three times the Message Time.
- **Neighbor Message Time (Sec)**—Displays the time between UDLD messages.

11

Smartport

This document describes the Smartports feature.

It contains the following topics:

- **Overview**
- **What is a Smartport**
- **Smartport Types**
- **Smartport Macros**
- **Macro Failure and the Reset Operation**
- **How the Smartport Feature Works**
- **Auto Smartport**
- **Error Handling**
- **Default Configuration**
- **Relationships with Other Features and Backwards Compatibility**
- **Common Smartport Tasks**
- **Configuring Smartport Using The Web-based Interface**
- **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 is a script of CLI (Command Line Interface) commands

A Smartport macro can be applied to an interface by the macro name, or by the Smartport type associated with the macro. Applying a Smartport macro by macro name can be done only through CLI. Refer to the CLI guide for details.

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

- **Static Smartport**—You manually assign 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 device. 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 (or user-defined) macro may be applied. These macros are designed to provide a means of quickly configuring the device 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 device 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.

You can apply a Smartport macro by the following methods:

- The associated Smartport type.

- Statically from a Smartport macro by name only from the CLI.

A Smartport macro can be applied by its Smartport type statically from CLI and 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.

The following describes the relationship of Smartport types and Auto Smartport

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
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 describe these 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 is re-initialized to Default in the following cases:

- A link down/up operation is performed on the interface.
- The device 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 you correct the error and applies the Reset action (performed in the Interface Settings pages) 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 is run, and the Smartport type returns to default.

Smartport Macros

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

Smartport macros should not be confused with global macros. Global macros configure the device 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 running the show parser macro name [macro_name] command in privileged exec mode of the CLI or 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.

There are two types of Smartport macros:

- **Built-In—**These are macros provided by the system. One macro applies the configuration profile and the other removes it. The macro names of the built-in Smartport macros and the Smartport type they are associated with as follows
  - macro-name (for example: printer)
  - no_macro-name (for example: no_printer)
- **User-Defined—**These are macros written by the users. See the CLI Reference Guide for more information about these. To associate a user defined macro to a Smartport type, its anti macro must be defined as well.
  - smartport-type-name (for example: my_printer)
  - no_smartport-type-name (for example: no_my_printer)

Smartport macros are bound to Smartport types in the Edit Smartport Type Setting page.

See **Built-in Smartport Macros** 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 device applies 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 might 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 pages). 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 macro name, or by the Smartport type associated with the macro. Applying a Smartport macro by macro name can be done only through the CLI, you should refer to the CLI guide for details.

Because support is provided for Smartport types which correspond to devices that 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 a Smartport macro by Smartport type to an interface:

- **Static Smartport**

  You manually assign 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 interface 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 relevant 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

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 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 must enable Auto Smartport at the desired interface as well. By default, Auto Smartport is enabled at all the interfaces.

See **Voice VLAN** 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 device 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 device 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 is 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 device detects the type of device attached to the port, based on the CDP/LLDP capabilities.

This mapping is shown in the following tables:

CDP Capabilities Mapping to Smartport Type

Capability Name	CDP Bit	Smartport Type
Router	0x01	Router
TB Bridge	0x02	Wireless Access Point

CDP Capabilities Mapping to Smartport Type (Continued)

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

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

LLDP Capabilities Mapping to Smartport Type (Continued)

Capability Name	LLDP Bit	Smartport Type
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 device 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 device through one interface, Auto Smartport considers 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 remains on the interface even after the attaching device ages out, the interface goes down, and the device is rebooted (assuming the configuration was saved). The Smartport type and the configuration of the interface are not changed unless Auto Smartport detects an attaching device with a different Smartport type. 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 device is rebooted. Enabling Persistent status on an interface eliminates the device detection delay that otherwise occurs.

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 is 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 and Interface Settings Edit pages.

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 **Voice VLAN** 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.

NOTE When upgrading from a firmware version 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 device, and to configure a port with Auto Smartport, perform the following steps:

STEP 1 To enable the Auto Smartport feature on the device, open the Smartport > Properties page. Set **Administrative Auto Smartport** to **Enable** or **Enable by Voice VLAN**.

STEP 2 Select whether the device is to process CDP and/or LLDP advertisements from connected devices.

STEP 3 Select which type of devices are to 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 and/or bind a user-defined macro pair to a Smartport type, 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.
- Bind a user-defined macro pair (a macro and its corresponding anti-macro) to a Smartport type.

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 bind user-defined macros to the selected Smartport type and/or modify the default values of the parameters in the macros bound to that Smartport type. These parameter default values are 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. Consider the troubleshooting tip below.

STEP 4 Click **Edit.** A new window appears in which you can click **Reset** to reset the interface.

STEP 5 Return to the main page and reapply the macro using either **Reapply** (for devices that are not switches, routers or APs) or **Reapply Smartport Macro** (for switches, routers or APs) to run the Smartport Macro on 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**. Then reapply the macro as described above.

TIP The reason that the macro failed might be a conflict with a configuration on the interface made prior to applying the macro (most often encountered with security and storm-control settings), a wrong port type, a typo or an 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.

Configuring Smartport Using The Web-based Interface

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

For Voice VLAN configuration, see **Voice VLAN**.

For LLDP/CDP configuration, see the **Configuring LLDP** and **Configuring CDP** sections, respectively.

Smartport Properties

To configure the Smartport feature globally:

STEP 1 Click **Smartport > Properties**.

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 Auto Voice VLAN*—This enables Auto Smartport, but puts 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—**Displays the Auto Smartport status.
- **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 does not assign that Smartport type to any interface.

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

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 **Smartport Types** for further information on macro versus anti-macro. Alternatively, you can associate your own pair of user-defined macros with customized configurations to a Smartport type. User-defined macros can be prepared only through CLI. You should refer to the CLI reference guide for details.

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 are used by Auto Smartport.

NOTE Changes to Auto Smartport types 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 causes all ports of this Smartport type to become unknown.

STEP 1 Click **Smartport > Smartport Type Settings**.

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 or assign a user-defined macro, select a Smartport type and click **Edit**.

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 Type**—Select whether the pair of macro and anti-macro associated with this Smartport type is built-in or user-defined.
- **User Defined Macro**—If desired, select the user-defined macro that is to be associated with the selected Smartport type. The macro must have already been paired with an anti-macro.

  Pairing of the two macros is done by name and is described in the Smartport Macro section.
- **Macro Parameters**—Displays the following fields for three parameters in the macro:
  - *Parameter Name*—Name of parameter in macro.
  - *Parameter Value*—Current value of parameter in macro. This can be changed here.
  - *Parameter Description*—Description of parameter.

  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 automatically reapplies the macro to the interfaces currently assigned with the Smartport type by Auto Smartport. Auto Smartport does 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.

Smartport 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 that failed upon application, and caused the Smartport type to become Unknown.
- Reapply a Smartport macro after it fails for one of the following types of interfaces: switch, router and AP. 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.
- Reapply a Smartport macro 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 device interface makes the interface a member of the VLANs created since the last macro application. You have to be familiar with the current configurations on the device and the definition of the macro to determine if a reapplication has any impact on the interface.
- Reset unknown interfaces. This sets the mode of Unknown interfaces to Default.

To apply a Smartport macro:

STEP 1 Click **Smartport > Interface Settings**.

Reapply the associated Smartport macro in the following ways:

- Select a group of Smartport types (switches, routers or APs) and click **Reapply Smartport Macro.** The macros are applied to all selected interface types.
- Select an interface that is UP and click **Reapply** to reapply the last macro that was applied to the interface.

The **Reapply** action also adds the interface to all newly-created VLANs.

STEP 2 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 displays the command at which application of the macro failed. See the workflow area in **Common Smartport Tasks** section for troubleshooting tips. Proceed to reapply the macro after correcting the problem.

STEP 3 Resetting all Unknown interfaces to Default type.

- Select the *Port Type equals to* checkbox.
- Select *Unknown* and click **Go.**
- Click **Reset All Unknown Smartports.** Then reapply the macro as described above. This performs a reset on all interfaces with type Unknown, meaning that all interfaces are returned 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**.

STEP 2 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 automatically assigns the Smartport type based on the CDP and/or LLDP advertisement received from the connecting devices as well as applying the 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 device 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 occurs.
- **Macro Parameters**—Displays the following fields for up to three parameters in the macro:
  - *Parameter Name*—Name of parameter in macro.
  - *Parameter Value*—Current value of parameter in macro. This can be changed here.
  - *Parameter Description*—Description of parameter.

STEP 3 Click **Reset** to set an interface to Default if it is in Unknown status (as a result of an unsuccessful macro application). The macro can be reapplied on the main page.

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
```

12

Port Management: PoE

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

This section describes how to use the PoE feature.

It covers the following topics:

- **PoE on the Device**
- **Configuring PoE Properties**
- **Configuring PoE Settings**

PoE on the Device

A PoE device 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.

See **Device Models** for information concerning PoE support on various models.

PoE Features

PoE provides the following features:

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

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

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

PoE Operation

PoE implements in the following stages:

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

PoE supports two modes:

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

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.

  NOTE Changing the mode from Class Limit to Port limit and vice versa when the device is operational forces the Powered Device to reboot.
- 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 device than the configured allocation allows (no matter if the device is in Class Limit or Port Limit mode), the device 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 an SNMP trap

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

The PoE models of the Sx200, Sx300, and SF500 series switches are PSE (Power Sourcing Equipment) that are capable of supplying DC power to attaching PD (Powered Devices). These devices include VoIP phones, IP cameras, and wireless access points. The PoE switches can detect and supply power to pre-standard legacy PoE Powered Devices. Due to the support of legacy PoE, it is possible that a PoE device acting as a PSE may mistakenly detect and supply power to an attaching PSE, including other PoE switches, as a legacy PD.

Even though Sx200/300/500 PoE switches are PSE, and as such should be powered by AC, they could be powered up as a legacy PD by another PSE due to false detection. When this happens, the PoE device may not operate properly and may not be able to properly supply power to its attaching PDs.

To prevent false detection, you should disable PoE on the ports on the PoE switches that are used to connect to PSEs. You should also first power up a PSE device before connecting it to a PoE device. When a device is being falsely detected as a PD, you should disconnect the device from the PoE port and power recycle the device with AC power before reconnecting its PoE ports.

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 device and monitor current power usage:

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

STEP 2 Enter the values for the following fields:

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

  NOTE When you change from Port Limit to Class Limit or vice versa, you must disable PoE ports, and enable them after changing the power configuration.

- **Traps**—Enable or disable traps. If traps are enabled, you must also enable SNMP and configure at least one SNMP Notification Recipient.
- **Power Trap Threshold**—Enter the usage threshold that is a percentage of the power limit. An alarm is initiated if the power exceeds this value.

The following counters are displayed:

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

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

Configuring PoE Settings

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.

NOTE PoE can be configured on the device for a specific period. This feature enables you to define, per port, the days in the week and the hours that PoE is enabled. When the time range is not active, PoE is disabled. To use this feature, a time range must first be defined in the **<300-500>Time Range** page.

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

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.

PoE priority example:

Given: A 48 port device is supplying a total of 375 watts.

The administrator configures all ports to allocate up to 30 watts. This results in 48 times 30 ports equaling 1440 watts, which is too much. The device cannot provide enough power to each port, so it provides power according to the priority.

The administrator sets the priority for each port, allocating how much power it can be given.

These priorities are entered in the PoE Settings page.

See **Device Models** for a description of the device 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.**The list of fields below is for Port Limit Power Mode. The fields are slightly different if the Power Mode is Class Limit.

STEP 2 Select a port and click **Edit.** The list of fields below is for Port Limit Power Mode. The fields are slightly different if the Power Mode is Class Limit.

STEP 3 Enter the value for the following field:

- **Interface**—Select the port to configure.
- **PoE Administrative Status**—Enable or disable PoE on the port.
- **Time Range**—Select to enabled PoE on the port.
- **Time Range Name**—If Time Range has been enabled, select the time range to be used. Time ranges are defined in the **<300-500>Time Range** page.
- **Power Priority Level**—Select the port priority: low, high, or critical, for use when the power supply is low. For example, if the power supply is running at 99% usage and port 1 is prioritized as high, but port 3 is prioritized as low, port 1 receives power and port 3 might be denied power.
- **Administrative Power Allocation**—This field appears 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.
- **Max Power Allocation**—This field appears only if the Power Mode set in the PoE Properties page is Power Limit. Displays the maximum amount of power permitted on this port.

- **Class**—This field appears 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 Device Port
0	15.4 watt
1	4.0 watt
2	7.0 watt
3	15.4 watt
4	30.0 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 written to the Running Configuration file.

13

VLAN Management

This section covers the following topics:

- **VLANs**
- **Configuring Default VLAN Settings**
- **Creating VLANs**
- **Configuring VLAN Interface Settings**
- **Defining VLAN Membership**
- **GVRP Settings<300-500 >**
- **VLAN Groups<300-500>**
- **Voice VLAN**
- **Access Port Multicast TV VLAN**
- **Customer Port Multicast TV VLAN<300-500>**

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. The tag contains a VLAN ID between 1 and 4094, and a VLAN Priority Tag (VPT) between 0 and 7. See **Quality of Service** 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

VLANs function at Layer 2. 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. Devices from different VLANs can communicate with each other only through Layer 3 routers. An IP router, for example, is required to route IP traffic between VLANs if each VLAN represents an IP subnet.

The IP router might be a traditional router, where each of its interfaces connects to only one VLAN. Traffic to and from a traditional IP router must be VLAN untagged. The IP router can be a VLAN-aware router, where each of its interfaces can connect to one or more VLANs. Traffic to and from a VLAN-aware IP router can be VLAN tagged or untagged.

Adjacent VLAN-aware devices exchange VLAN information with each other by using Generic VLAN Registration Protocol (GVRP). As a result, VLAN information is propagated through a bridged network.

VLANs on a device can be created statically or dynamically, based on the GVRP information exchanged by devices. A VLAN can be static or dynamic (from GVRP), but not both. For more information about GVRP, refer to the GVRP Settings section.

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 (in Layer 2-system-mode systems): For more information refer to the Layer 2 IP Addressing section.

QinQ

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

With QinQ, the device 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 device 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. This is only relevant for OUI-enabled voice VLAN.
- If a port is no longer a member of any VLAN, the device automatically configures the port as an untagged member of the default VLAN. A port is no longer a member of a VLAN if the VLAN is deleted or the port is removed from the VLAN.
- RADIUS servers cannot assign the default VLAN to 802.1x supplicants by using Dynamic VLAN Assignment.

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

- 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 device. 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**.

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 device.

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 300 Series device supports up to 4K VLANs, including the default VLAN.

Each VLAN must be configured with a unique VID (VLAN ID) with a value from 1 to 4094. The device 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** > **VLAN Settings**.

This page displays the following fields for all VLANs:

- **VLAN ID**—User-defined VLAN ID.
- **VLAN Name**—User-defined VLAN name.
- **Originators**—VLAN type:
  - *GVRP*—VLAN was dynamically created through Generic VLAN Registration Protocol (GVRP).
  - *Static*—VLAN is user-defined.
  - *Default*—VLAN is the default VLAN.

STEP 2 Click **Add** to add a new VLAN.

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.**

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

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

STEP 4 Enter the values for the following fields:

- **Interface**—Select a Port/LAG.
- **Interface VLAN Mode**—Select the interface mode for the VLAN. The options are:
    - *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 you to use your own VLAN arrangements (PVID) across the provider network. The device is in Q-in-Q mode when it has one or more 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 the packets properly, intermediate VLAN-aware devices that carry VLAN traffic along the path between end nodes must either be manually configured or must dynamically learn the VLANs and their port memberships from Generic VLAN Registration Protocol (GVRP).

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

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

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**.

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 appears with its current port mode (Access, Trunk, General or Customer) configured from the Interface Settings page.

Each port or LAG appears 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 even from GVRP registration. When a port is not a member of any other VLAN, enabling this option on the port makes the port part of internal VLAN 4095 (a reserved VID).
- **Excluded**—The interface is currently not a member of the VLAN. This is the default for all the ports and LAGs. The port can join the VLAN through GVRP registration.
- **Tagged**—The interface is a tagged member of the VLAN.
- **Untagged**—The interface is an untagged member of the VLAN. Frames of the VLAN are sent untagged to the interface VLAN.
- **Multicast TV VLAN**—The interface used for Digital TV using Multicast IP. The port joins the VLAN with a VLAN tag of Multicast TV VLAN. See **Access Port Multicast TV VLAN** for more information.
- **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 is marked with an upper case 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**.

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.

STEP 4 Enter the values for the following fields:

- **Interface**—Select a Port or LAG.
- **Mode**—Displays the port VLAN mode that was selected in the Interface Settings page.
- **Select VLAN**—To associate a port with a VLAN(s), move the VLAN ID(s) from the left list to the right list by using the arrow buttons. The default VLAN might appear in the right list if it is tagged, but it cannot be selected.
- **Tagging**—Select one of the following tagging/PVID options:

- **Tagged**—Select whether the port is tagged. This is not relevant for Access ports.
- **Untagged**—Select whether port is untagged. This is not relevant for Access ports.
- **PVID**—Port PVID is set to this VLAN. If the interface is in access mode or trunk mode, the device 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.

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

GVRP Settings

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

Since GVRP requires support for tagging, the port must be configured in Trunk or General mode.

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

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

By default, GVRP is disabled globally and on ports.

Defining GVRP Settings

To define GVRP settings for an interface:

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

STEP 2 Select **GVRP Global Status** to enable GVRP globally.

STEP 3 Click **Apply** to set the global GVRP status.

STEP 4 Select an interface type (Port or LAG), and click **Go** to display all interfaces of that type.

STEP 5 To define GVRP settings for a port, select it, and click **Edit.**

STEP 6 Enter the values for the following fields:

- **Interface—**Select the interface (Port or LAG) to be edited.
- **GVRP State—**Select to enable GVRP on this interface.
- **Dynamic VLAN Creation—**Select to enable Dynamic VLAN Creation on this interface.
- **GVRP Registration—**Select to enable VLAN Registration using GVRP on this interface.

STEP 7 Click **Apply**. GVRP settings are modified, and written to the Running Configuration file.

VLAN Groups

VLAN groups are used for load balancing of traffic on a Layer 2 network.

Packets are assigned a VLAN according to various classifications that have been configured (such as VLAN groups).

If several classifications schemes are defined, packets are assigned to a VLAN in the following order:

- TAG: If the packet is tagged, the VLAN is taken from the tag.
- MAC-Based VLAN: If a MAC-based VLAN has been defined, the VLAN is taken from the source MAC-to-VLAN mapping of the ingress interface.

- **PVID:** VLAN is taken from the port default VLAN ID.

MAC-based Groups

MAC-based VLAN classification enable packets to be classified according to their source MAC address. You can then define MAC-to-VLAN mapping per interface.

You can define several MAC-based VLAN groups, which each group containing different MAC addresses.

These MAC-based groups can be assigned to specific ports/LAGs. MAC-based VLAN groups cannot contain overlapping ranges of MAC addresses on the same port.

The following table describes the availability of MAC-based VLAN groups in various SKUs:

Table 1 MAC-Based VLAN Group Availability

SKU	System Mode	MAC-based VLAN Groups Supported
Sx300	**Layer 2**	Yes
	Layer 3	No
Sx500, Sx500ESW2-550X	**Layer 2**	Yes
	Layer 3	No
SG500X	**Native**	Yes
	Basic Hybrid - Layer 2	Yes
	Basic Hybrid - Layer 3	No
SG500XG	**Same as Sx500**	Yes

Workflow

To define a MAC-based VLAN group:

1. Assign a MAC address to a VLAN group ID (using the MAC-Based Groups page).
2. For each required interface:

a. Assign the VLAN group to a VLAN (using Mac-Based Groups to VLAN page). The interfaces must be in General mode.

b. If the interface does not belong to the VLAN, manually assign it to the VLAN using the Port to VLAN page.

Assigning MAC-based VLAN Groups

See Table 1 for a description of the availability of this feature.

To assign a MAC address to a VLAN Group:

STEP 1 Click **VLAN Management** > **VLAN Groups** > **MAC-Based Groups**.

STEP 2 Click **Add.**

STEP 3 Enter the values for the following fields:

- **MAC Address**—Enter a MAC address to be assigned to a VLAN group.

  NOTE This MAC address cannot be assigned to any other VLAN group.

- **Mask**—Enter one of the following:
  - *Host*—Source host of the MAC address
  - *Length*—*Prefix* of the MAC address
- **Group ID**—Enter a user-created VLAN group ID number.

STEP 4 Click **Apply**. The MAC address is assigned to a VLAN group.

Mapping VLAN Group to VLAN Per Interface

See Table 1 for a description of the availability of this feature.

Ports/LAGs must be in General mode.

To assign a MAC-based VLAN group to a VLAN on an interface:

STEP 1 Click **VLAN Management** > **VLAN Groups** > **MAC-Based Groups to VLAN.**

STEP 2 Click **Add.**

STEP 3 Enter the values for the following fields:

- **Group Type**—Displays that the group is MAC-Based.

- **Interface—**Enter a general interface (port/LAG) through which traffic is received.
- **Group ID—**Select a VLAN group, defined in the MAC-Based Groups page.
- **VLAN ID—**Select the VLAN to which traffic from the VLAN group is forwarded.

STEP 4 Click **Apply** to set the mapping of the VLAN group to the VLAN. This mapping does not bind the interface dynamically to the VLAN; the interface must be manually added to the VLAN.)

Protocol-based VLANs

Groups of protocols can be defined and then bound to a port. After the protocol group is bound to a port, every packet originating from a protocol in the group is assigned the VLAN that is configured in the Protocol-Based Groups page.

Workflow

To define a protocol-based VLAN group:

1. Define a protocol group (using the Protocol-Based Groups page).
2. For each required interface, assign the protocol group to a VLAN (using Protocol-Based Groups to VLAN page). The interfaces must be in General mode and cannot have a Dynamic VLAN (DVA) assigned to it.

Protocol-Based Groups

To define a set of protocols.

STEP 1 Click VLAN Management > **VLAN Groups** > Protocol-Based Groups.

The Protocol-Based Groups Page contains the following fields:

- Encapsulation—Displays the protocol on which the VLAN group is based.
- Protocol Value (Hex)—Displays the protocol value in hex.
- Group ID—Displays the protocol group ID to which the interface is added.

STEP 2 Click the Add Button. The Add Protocol-Based Group page appears

STEP 3 Enter the following fields:.

- **Encapsulation**—Protocol Packet type. The following options are available:
    - *Ethernet V2*—If this is selected, select the **Ethernet Type.**
    - *LLC-SNAP (rfc1042)*—If this is selected, enter the **Protocol Value.**
    - *LLC*—If this is selected, select the **DSAP-SSAP Values.**
- **Ethernet Type**—Select the Ethernet type for Ethernet V2 encapsulation. This is the two-octet field in the Ethernet frame used to indicate which protocol is encapsulated in the payload of the Ethernet packet) for the VLAN group
- **Protocol Value**—Enter the protocol for LLC-SNAP (rfc 1042)encapsulation.
- **DSAP-SSAP**—Enter these values for LLC encapsulation.
- **Group ID**—Enter a protocol group ID.

STEP 4 Click **Apply.** The Protocol Group is added, and written to the Running Configuration file.

Protocol-Based Groups to VLAN Mapping

To map a protocol group to a port, the port must be in General mode and not have DVA configured on it (see **Configuring VLAN Interface Settings**).

Several groups can be bound to a single port, with each port being associated to its own VLAN.

It is possible to map several groups to a single VLAN as well.

To map the protocol port to a VLAN:

STEP 1 Click **VLAN Management** > **VLAN Groups** > **Protocol-Based Groups to VLAN.**

The currently-defined mappings are displayed.

STEP 2 To associate an interface with a protocol-based group and VLAN, click **Add.**

STEP 3 Enter the following fields.

- **Interface**—Port or LAG number assigned to VLAN according to protocol-based group.
- **Group ID**—Protocol group ID.
- **VLAN ID**—Attaches the interface to a user-defined VLAN ID.

STEP 4 Click **Apply**. The protocol ports are mapped to VLANs, and written to the Running Configuration file.

Voice VLAN

In a LAN, voice devices, such as IP phones, VoIP endpoints, and voice systems are placed into the same VLAN. This VLAN is referred as the voice VLAN. If the voice devices are in different voice VLANs, IP (Layer 3) routers are needed to provide communication.

This section covers the following topics:

- **Voice VLAN Overview**
- **Configuring Voice VLAN**

Voice VLAN Overview

This section covers 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 device always operates as a VLAN-aware switch.

The device supports a single voice VLAN. By default, the voice VLAN is VLAN 1. 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 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 device is in Telephony OUI mode, or has Auto Smartports enabled.

Dynamic Voice VLAN Modes

The device supports two dynamic voice VLAN modes: 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 device is in Telephony OUI mode and a port is manually configured as a candidate to join the voice VLAN, the device 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 **Configuring Telephony OUI**.

- **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 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 Cisco 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 device 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 device 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 the Dynamic Voice VLAN mode is Enable Auto Voice VLAN, Auto Voice VLAN becomes 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 the Voice VLAN Discovery Protocol (VSDP). If desired, you can activate Auto Voice VLAN immediately without waiting for a trigger.

When Auto Smartport is enabled, depending on Auto Voice VLAN mode, Auto Smartport is enabled when Auto Voice VLAN becomes operational. If desired, you can make 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 Unified Communication (UC) devices, are advertising their voice VLAN, the voice VLAN from the device with the lowest MAC address is used.

  NOTE If connecting the device 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 device 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 user. When restarted, the device 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 device 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 device is in Layer 2 system mode, it can synchronize with only VSDP capable switches in the same management VLAN. If the device is in Layer 3 system mode, it can synchronize with VSDP capable switches that are in the directly-connected IP subnets configured at the device.

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 device 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 response with the Voice QoS setting if an appliance sends LLDP-MED packets. MED-supported devices must send their voice traffic with the same CoS/802.1p and DSCP values, as received with the LLDP-MED response.

You can disable the automatic update between Voice VLAN and LLDP-MED and use his own network policies.

Working with the OUI mode, the device can additionally configure the mapping and remarking (CoS/802.1p) of the voice traffic based on the OUI.

By default, all interfaces are CoS/802.1p trusted. The device applies the quality of service based on the CoS/802.1p value found in the voice stream. In Auto Voice VLAN, you can override the value of the voice streams using advanced QoS. For Telephony OUI voice streams, you can override the quality of service and optionally remark the 802.1p of the voice streams by specifying the desired CoS/802.1p values and using the remarking option under Telephony OUI.

Voice VLAN 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.
- The Voice VLAN cannot support DVA (Dynamic VLAN assignment).
- The Voice VLAN cannot be the Guest VLAN if the voice VLAN mode is OUI. If the voice VLAN mode is Auto, then the Voice VLAN can be the Guest VLAN.
- The Voice VLAN QoS decision has priority over any other QoS decision, except for the Policy/ACL QoS decision.
- 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 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 device 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.

NOTE Step 7 and Step 8 are optional as they are enabled by default.

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 covers 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 voice VLAN settings configured on the device are displayed in the **Voice VLAN Settings (Administrative Status)** block.
- The voice VLAN settings that are actually being applied to the voice VLAN deployment are displayed in the **Voice VLAN Settings (Operational Status)** block.

STEP 2 Enter values for the following fields:

- **Voice VLAN ID**—Enter the VLAN that is to be the Voice VLAN.

  NOTE Changes in the voice VLAN ID, CoS/802.1p, and/or DSCP cause the device to advertise the administrative voice VLAN as a static voice VLAN. If the option *Auto Voice VLAN Activation* triggered by external Voice VLAN is selected, then the default values need to be maintained.

- **CoS/802.1p** —Select a CoS/802.1p value that to 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 to 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 device is to be activated and put into operation immediately if enabled.
    - *By External Voice VLAN Trigger*—Auto Voice VLAN on the device is activated and put into operation only if the device 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 results 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 only resets 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 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 device.
- **CoS/802.1p—**Displays CoS/802.1p values to be used by the LLDP-MED as a voice network policy.
- **DSCP—**Displays DSCP values to 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 device. 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 displays voice VLAN configured on the device, as well as any voice VLAN configuration advertised by directly-connected neighbor devices. It contains the following fields:

- **Interface—**Displays the interface on which voice VLAN configuration was received or configured. If N/A appears, the configuration was done on the device itself. If an interface appears, a voice configuration was received from a neighbor.
- **Source MAC Address—** MAC address of a UC from which the voice configuration was received.
- **Source Type—** Type of UC from which voice configuration was received. The following options are available:
  - *Default*—Default voice VLAN configuration on the device

  - *Static*—User-defined voice VLAN configuration defined on the device.
  - *CDP*—UC that advertised voice VLAN configuration is running CDP.
  - *LLDP*—UC that advertised voice VLAN configuration is running LLDP.
  - *Voice VLAN ID*—The identifier of the advertised or configured voice VLAN
- **Voice VLAN ID**—The identifier of the current voice VLAN.
- **CoS/802.1p**—The advertised or configured CoS/802.1p values that are used by the LLDP-MED as a voice network policy.
- **DSCP**—The advertised or configured DSCP values that are used by the LLDP-MED as a voice network policy.
- **Best Local Source**—Displays whether this voice VLAN was used by the device. The following options are available:
  - *Yes*—The device uses this voice VLAN to synchronize with other Auto Voice VLAN-enabled switches. This voice VLAN is 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 covers 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 contains 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 device with these values.

The Telephony OUI table appears:

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

STEP 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.**

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 contains voice VLAN OUI parameters for all interfaces.

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

STEP 3 Enter the values for the following fields:

- **Interface**—Select an interface.
- **Telephony OUI VLAN Membership**—If enabled, the interface is a candidate port of the telephony OUI based voice VLAN. When packets that match one of the configured telephony OUI are received, the port is added to the voice VLAN.
- **Telephone OUI QoS Mode**—Select one of the following options:
  - *All*—QoS attributes are applied on all packets that are classified to the Voice VLAN.
  - *Telephony Source MAC Address*—QoS attributes are applied only on packets from IP phones.

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

Access Port Multicast TV VLAN

Multicast TV VLANs enable Multicast transmissions to subscribers who are not on the same data VLAN (Layer 2-isolated), without replicating the Multicast transmission frames for each subscriber VLAN.

Subscribers, who are not on the same data VLAN (Layer 2-isolated) and are connected to the device with different VLAN ID membership. can share the same Multicast stream by joining the ports to the same Multicast VLAN ID.

The network port, connected to the Multicast server, is statically configured as a member in the Multicast VLAN ID.

The network ports, which through subscribers communicate with the Multicast server (by sending IGMP messages), receive the Multicast streams from the Multicast server, while including the Multicast TV VLAN in the Multicast packet header. For this reasons, the network ports must be statically configured as the following:

- Trunk or general port type (see **Configuring VLAN Interface Settings**)
- Member on the Multicast TV VLAN

The subscriber receiver ports can be associated with the Multicast TV VLAN only if it is defined in one of the two following types:

- Access port
- Customer port (see **Customer Port Multicast TV VLAN<300-500>**)

One or more IP Multicast address groups can be associated with the same Multicast TV VLAN.

Any VLAN can be configured as a Multicast-TV VLAN. A port assigned to a Multicast-TV VLAN:

- Joins the Multicast-TV VLAN.
- Packets passing through egress ports in the Multicast TV VLAN are untagged.

- The port’s Frame Type parameter is set to **Admit All**, allowing untagged packets (see **Configuring VLAN Interface Settings**).

The Multicast TV VLAN configuration is defined per port. Customer ports are configured to be member of Multicast TV VLANs using the Multicast TV VLAN Page.

IGMP Snooping

Multicast TV VLAN relies on IGMP snooping, which means that:

- Subscribers use IGMP messages to join or leave a Multicast group.
- Device performs IGMP snooping and configures the access port according to its Multicast membership on Multicast TV VLAN.

The device decides for each IGMP packet that is received on an access port whether to associate it with the access VLAN or with the Multicast TV VLAN according to the following rules:

- If an IGMP message is received on an access port, with destination Multicast IP address that is associated with the port’s Multicast TV VLAN, then the software associates the IGMP packet with the Multicast TV VLAN.
- Otherwise the IGMP message is associated to the access VLAN and the IGMP message is only forwarded within that VLAN.
- The IGMP message is discarded if:
    - The STP/RSTP state on the access port is **discard**.
    - The MSTP state for the access VLAN is **discard**.
    - The MSTP state for the Multicast TV VLAN is **discard**, and the IGMP message is associated with this Multicast TV VLAN.

Differences Between Regular and Multicast TV VLANs

Characteristics of Regular vs. Multicast TV VLANs

	Regular VLAN	Multicast TV VLAN
VLAN Membership	Source and all receiver ports must be static members in the same data VLAN.	Source and receiver ports cannot be members in the same data VLAN.

	Regular VLAN	Multicast TV VLAN
Group registration	All Multicast group registration is dynamic.	Groups must be associated to Multicast VLAN statically, but actual registration of station is dynamic.
Receiver ports	VLAN can be used to both send and receive traffic (both Multicast and Unicast).	Multicast VLAN can only be used to receive traffic by the stations on the port (only Multicast).
Security and Isolation	Receivers of same multicast stream are on the same data VLAN and can communicate with each other	Receivers of same multicast stream are in different Access VLANs and isolated from each other

Configuration

Workflow

Configure TV VLAN with the following steps:

1. Define a TV VLAN by associating a Multicast group to a VLAN (using the Multicast Group to VLAN page).
2. Specify the access ports in each Multicast VLAN (using the Port Multicast VLAN Membership page.

Multicast TV Group to VLAN

To define the Multicast TV VLAN configuration:

STEP 1 Click **VLAN Management** > **Access Port Multicast TV VLAN > Multicast Group to VLAN.**

The following fields are displayed:

- **Multicast Group—**IP address of the Multicast group.
- **Multicast TV VLAN—**VLAN to which the Multicast packets are assigned.

STEP 2 Click **Add** to associate a Multicast group to a VLAN. Any VLAN can be selected. When a VLAN is selected, it becomes a Multicast TV VLAN.

STEP 3 Click **Apply.** Multicast TV VLAN settings are modified, and written to the Running Configuration file.

Port Multicast VLAN Membership

To define the Multicast TV VLAN configuration:

STEP 1 Click **VLAN Management** > **Access Port Multicast TV VLAN** > **Port Multicast VLAN Membership.**

STEP 2 Select a VLAN from the **Multicast TV VLAN** field.

STEP 3 The **Candidate Access Ports** list contains all access ports configured on the device. Move the required ports from the **Candidate Access Ports** field to the **Member Access Ports** field.

STEP 4 Click **Apply.** Multicast TV VLAN settings are modified, and written to the Running Configuration file.

Customer Port Multicast TV VLAN

A triple play service provisions three broadband services, over a single broadband connection:

- High-speed Internet access
- Video
- Voice

The triple play service is provisioned for service provider subscribers, while keeping Layer 2-isolation between them.

Each subscriber has a CPE MUX box. The MUX has multiple access ports that are connected to the subscriber's devices (PC, telephone and so on), and one network port that is connected to the access device.

The box forwards the packets from the network port to the subscriber's devices based on the VLAN tag of the packet. Each VLAN is mapped to one of the MUX access ports.

Packets from subscribers to the service provider network are forwarded as VLAN tagged frames, in order to distinguish between the service types, which mean that for each service type there is a unique VLAN ID in the CPE box.

All packets from the subscriber to the service provider network are encapsulated by the access device with the subscriber's VLAN configured as customer VLAN (Outer tag or S-VID), except for IGMP snooping messages from the TV receivers, which are associated with the Multicast TV VLAN. VOD information that is also sent from the TV receivers are sent like any other type of traffic.

Packets from the service provider network that received on the network port to the subscriber are sent on the service provider network as double tag packets, while the outer tag (Service Tag or S-Tag) represent one of the two type of VLAN as following:

- Subscriber's VLAN (Includes Internet and IP Phones)
- Multicast TV VLAN

The inner VLAN (C-Tag) is the tag that determines the destination in the subscriber's network (by the CPE MUX).

Workflow

1. Configure an access port as a customer port (using the VLAN Management > Interface Settings page). See **QinQ** for more information.
2. Configure the network port as a trunk or general port with subscriber and Multicast TV VLAN as tagged VLANS. (using the VLAN Management > Interface Settings page.
3. Create a Multicast TV VLAN with up to 4094 different VLAN(s). (The VLAN creation is done via the regular VLAN management configuration)
4. Associate the customer port to a Multicast TV VLAN, using the Port Multicast VLAN Membership page.
5. Map the CPE VLAN (C-TAG) to the Multicast TV VLAN (S-Tag), using the CPE VLAN to VLAN page.

Mapping CPE VLANs to Multicast TV VLANs

To support the CPE MUX with subscribers VLANs, subscribers may require multiple video providers, and each provider is assigned a different external VLAN.

CPE (internal) Multicast VLANs must be mapped to the Multicast provider (external) VLANs.

After a CPE VLAN is mapped to a Multicast VLAN, it can participate in IGMP snooping.

To map CPE VLANs:

STEP 1 Click **VLAN Management** > **Customer Port Multicast TV VLAN** > **CPE VLAN to VLAN.**

STEP 2 Click **Add.**

STEP 3 Enter the following fields:

- **CPE VLAN**—Enter the VLAN defined on the CPE box.
- **Multicast TV VLAN**—Select the Multicast TV VLAN which is mapped to the CPE VLAN.

STEP 4 Click **Apply.** CPE VLAN Mapping is modified, and written to the Running Configuration file.

CPE Port Multicast VLAN Membership

The ports associated with the Multicast VLANs must be configured as customer ports (see **Configuring VLAN Interface Settings**).

Use the Port Multicast VLAN Membership page to map these ports to Multicast TV VLANs as described in **Port Multicast VLAN Membership**

14

Spanning Tree

This section describes the Spanning Tree Protocol (STP) (IEEE802.1D and IEEE802.1Q) and covers the following topics:

- **STP Flavors**
- **Configuring STP Status and Global Settings**
- **Defining Spanning Tree Interface Settings**
- **Configuring Rapid Spanning Tree Settings**
- **Multiple Spanning Tree**
- **Defining MSTP Properties**
- **Mapping VLANs to a MSTP Instance**
- **Defining MSTP Instance Settings**
- **Defining MSTP Interface Settings**

STP Flavors

STP protects a Layer 2 Broadcast domain from Broadcast storms by selectively setting links to standby mode to prevent loops. In standby mode, these links temporarily stop transferring user data. After the topology changes so that the data transfer is made possible, the links are automatically re-activated.

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

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

The device 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.
- Multiple STP (MSTP) – MSTP is based on RSTP. It detects Layer 2 loops, and attempts to mitigate them by preventing the involved port from transmitting traffic. Since loops exist on a per-Layer 2-domain basis, a situation can occur where there is a loop in VLAN A and no loop in VLAN B. If both VLANs are on Port X, and STP wants to mitigate the loop, it stops traffic on the entire port, including VLAN B traffic.

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

Configuring STP Status and Global Settings

The STP Status and Global Settings page contains parameters for enabling STP, RSTP, or MSTP.

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

To set the STP status and global settings:

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

STEP 2 Enter the parameters.

Global Settings:

- **Spanning Tree State**—Enable or disable STP on the device.
- **STP Operation Mode—**Select an STP mode.

- **BPDU Handling**—Select how Bridge Protocol Data Unit (BPDU) packets are managed when STP is disabled on the port or the device. 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 the Root Bridge. The bridge priority value is provided in increments of 4096. For example, 4096, 8192, 12288, and so on.
- **Hello Time**—Set the interval (in seconds) that a Root Bridge waits between configuration messages.
- **Max Age**—Set the interval (in seconds) that the device can wait without receiving a configuration message, before attempting to redefine its own configuration.
- **Forward Delay**—Set the interval (in seconds) that a bridge remains in a learning state before forwarding packets. For more information, refer to **Defining Spanning Tree Interface Settings**.

Designated Root:

- **Bridge ID**—The bridge priority concatenated with the MAC address of the device.
- **Root Bridge ID**—The Root Bridge priority concatenated with the MAC address of the Root Bridge.
- **Root Port**—The port that offers the lowest cost path from this bridge to the Root Bridge. (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 appears in a days/hours/minutes/ seconds format.

STEP 3 Click **Apply**. The STP Global settings are written to the Running Configuration file.

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 defined configuration entered is valid for all flavors of the STP protocol.

To configure STP on an interface:

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

STEP 2 Select an interface and click **Edit**.

STEP 3 Enter the parameters

- **Interface—**Select the Port or LAG on which Spanning Tree is configured.
- **STP—**Enables or disables STP on the port.
- **Edge Port—**Enables or disables Fast Link on the port. If Fast Link mode is enabled on a port, the port is automatically set to Forwarding state when the port link is up. Fast Link optimizes the STP protocol convergence. The options are:
    - *Enable*—Enables Fast Link immediately.
    - *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.

    NOTE It is recommended to set the value to Auto so that the device sets the port to fast link mode if a host is connected to it, or sets it as a regular STP port if connected to another device. This helps avoid loops.

- **Root Guard**—Enables or disables Root Guard on the device. The Root Guard option provides a way to enforce the root bridge placement in the network.

  Root Guard ensures that the port on which this feature is enabled is the designated port. Normally, all root bridge ports are designated ports, unless two or more ports of the root bridge are connected. If the bridge receives superior BPDUs on a Root Guard-enabled port, Root Guard moves this port to a root-inconsistent STP state. This root-inconsistent state is effectively equal to a listening state. No traffic is forwarded across this port. In this way, Root Guard enforces the position of the root bridge.

- **BPDU Guard**—Enables or disables the Bridge Protocol Data Unit (BPDU) Guard feature on the port.

  The BPDU Guard enables you to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have BPDU Guard enabled cannot influence the STP topology. At the reception of BPDUs, the BPDU guard operation disables the port that has BPDU configured. In this case, a BPDU message is received, and an appropriate SNMP trap is generated.

- **BPDU Handling**—Select how BPDU packets are managed when STP is disabled on the port or the device. 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 written to the Running Configuration file.

Configuring Rapid Spanning Tree Settings

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

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

To enter RSTP settings:

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

STEP 2 Click **Spanning Tree** > **RSTP Interface Settings**. The RSTP Interface Settings page appears:

STEP 3 Select a port.

NOTE Activate Protocol Migration is only available after selecting the port that is 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 or MSTP. If it still exists as an STP link, the device continues to communicate with it by using STP. Otherwise, if it has been migrated to RSTP or MSTP, the device communicates with it using RSTP or MSTP, respectively.

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

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 an RSTP edge port when this feature is enabled, and is brought 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 high speed.
  - *Auto*—Automatically determines the device status by using RSTP BPDUs.
- **Point to Point Operational Status—**Displays the Point-to-Point operational status if the **Point to Point Administrative Status** is set to Auto.
- **Role—**Displays the role of the port that was assigned by STP to provide STP paths. The possible roles are:
  - *Root*—Lowest cost path to forward packets to the Root Bridge.

  - *Designated*—The interface through which the bridge is connected to the LAN, which provides the lowest cost path from the LAN to the Root Bridge.
  - *Alternate*—Provides an alternate path to the Root Bridge from the root interface.
  - *Backup*—Provides a backup path to the designated port path toward the Spanning Tree leaves. This provides a configuration in which two ports are connected in a loop by a point-to-point link. Backup ports are also used when a LAN has two or more established connections to a shared segment.
  - *Disabled*—The port is not participating in Spanning Tree.
- **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.

Multiple Spanning Tree

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

To configure MSTP:

1. Set the STP Operation Mode to MSTP as described in the **Configuring STP Status and Global Settings** page*.*
2. Define MSTP instances. Each MSTP instance calculates and builds a loop free topology to bridge packets from the VLANs that map to the instance. Refer to t*he* **Mapping VLANs to a MSTP Instance** section.
3. Decide which MSTP instance be active in what VLAN, and associate these MSTP instances to VLAN(s) accordingly.
4. Configure the MSTP attributes by:
    - **Defining MSTP Properties**
    - **Defining MSTP Instance Settings**
    - **Mapping VLANs to a MSTP Instance**

Defining MSTP Properties

The global MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree instance. MSTP enables formation of MST regions that can run multiple MST instances (MSTI). Multiple regions and other STP bridges are interconnected using one single common spanning tree (CST).

MSTP is fully compatible with RSTP bridges, in that an MSTP BPDU can be interpreted by an RSTP bridge as an RSTP BPDU. This not only enables compatibility with RSTP bridges without configuration changes, but also causes any RSTP bridges outside of an MSTP region to see the region as a single RSTP bridge, regardless of the number of MSTP bridges inside the region itself.

For two or more switches to be in the same MST region, they must have the same VLANs to MST instance mapping, the same configuration revision number, and the same region name.

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

This mapping can be done in the VLAN to MST Instance page.

Use this page if the system operates in MSTP mode.

To define MSTP:

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

STEP 2 Click **Spanning Tree** > **MSTP Properties**.

STEP 3 Enter the parameters.

- **Region Name—**Define an MSTP region name.
- **Revision—**Define an unsigned 16-bit number that identifies the revision of the current MST configuration. The field range is from 0 to 65535.
- **Max Hops**—Set the total number of hops that occur in a specific region before the BPDU is discarded. Once the BPDU is discarded, the port information is aged out. The field range is from 1 to 40.
- **IST Master**—Displays the regions master.

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

Mapping VLANs to a MSTP Instance

The VLAN to MSTP Instance page enables you to map each VLAN to a Multiple Spanning Tree Instance (MSTI). For devices to be in the same region, they must have the same mapping of VLANs to MSTIs.

NOTE The same MSTI can be mapped to more than one VLAN, but each VLAN can only have one MST Instance attached to it.

Configuration on this page (and all of the MSTP pages) applies if the system STP mode is MSTP.

Up to seven MST instances (predefined from 1-7) can be defined on 300 Series switches, in addition to instance zero.

For those VLANs that are not explicitly mapped to one of the MST instances, the device automatically maps them to the CIST (Core and Internal Spanning Tree) instance. The CIST instance is MST instance 0.

To map VLANs to MST Instances:

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

The VLAN to MSTP Instance page contains the following fields:

- **MST Instance ID—**All MST instances are displayed.
- **VLANs—**All VLANs belonging to the MST instance are displayed.

STEP 2 To add a VLAN to an MSTP instance, select the MST instance, and click **Edit**.

STEP 3 Enter the parameters.

- **MST Instance ID—**Select the MST instance.
- **VLANs—**Define the VLANs being mapped to this MST instance.
- **Action—**Define whether to **Add** (map) the VLAN to the MST instance or **Remove** it.

STEP 4 Click **Apply**. The MSTP VLAN mappings are defined, and the Running Configuration file is updated.

Defining MSTP Instance Settings

The MSTP Instance Settings page enables you to configure and view parameters per MST instance. This is the per-instance equivalent to the *Configuring STP Status and Global Settings*.

To enter MSTP instance settings:

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

STEP 2 Enter the parameters.

- **Instance ID—**Select an MST instance to be displayed and defined.

- **Included VLAN**—Displays the VLANs mapped to the selected instance. The default mapping is that all VLANs are mapped to the common and internal spanning tree (CIST) instance 0).
- **Bridge Priority**—Set the priority of this bridge for the selected MST instance.
- **Designated Root Bridge ID**—Displays the priority and MAC address of the Root Bridge for the MST instance.
- **Root Port**—Displays the root port of the selected instance.
- **Root Path Cost**—Displays the root path cost of the selected instance.
- **Bridge ID**—Displays the bridge priority and the MAC address of this device for the selected instance.
- **Remaining Hops**—Displays the number of hops remaining to the next destination.

STEP 3 Click **Apply**. The MST Instance configuration is defined, and the Running Configuration file is updated.

Defining MSTP Interface Settings

The MSTP Interface Settings page enables you to configure the port MSTP settings for every MST instance, and to view information that has currently been learned by the protocol, such as the designated bridge per MST instance.

To configure the ports in an MST instance:

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

STEP 2 Enter the parameters.

- **Instance equals To**—Select the MSTP instance to be configured.
- **Interface Type equals to**—Select whether to display the list of ports or LAGs.

STEP 3 Click **Go**. The MSTP parameters for the interfaces on the instance are displayed.

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

STEP 5 Enter the parameters.

- **Instance ID**—Select the MST instance to be configured.
- **Interface**—Select the interface for which the MSTI settings are to be defined.
- **Interface Priority**—Set the port priority for the specified interface and MST instance.
- **Path Cost**—Enter the port contribution to the root path cost in the **User Defined** textbox or select **Use Default** to use the default value.
- **Port State**—Displays the MSTP status of the specific port on a specific MST instance. The parameters are defined as:
    - *Disabled*—STP is currently disabled.
    - *Blocking*—The port on this instance is currently blocked, and cannot forward traffic (with the exception of BPDU data) or learn MAC addresses.
    - *Listening*—The port on this instance is in Listening mode. The port cannot forward traffic, and cannot learn MAC addresses.
    - *Learning*—The port on this instance is in Learning mode. The port cannot forward traffic, but it can learn new MAC addresses.
    - *Forwarding*—The port on this instance is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
    - *Boundary*—The port on this instance is a boundary port. It inherits its state from instance 0 and can be viewed on the STP Interface Settings page.
- **Port Role**—Displays the port or LAG role, per port or LAG per instance, assigned by the MSTP algorithm to provide STP paths:
    - *Root*—Forwarding packets through this interface provides the lowest cost path for forwarding packets to the root device.
    - *Designated*—The interface through which the bridge is connected to the LAN, which provides the lowest root path cost from the LAN to the Root Bridge for the MST instance.
    - *Alternate*—The interface provides an alternate path to the root device from the root interface.

  - *Backup*—The interface provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more established connections to a shared segment.
  - *Disabled*—The interface does not participate in the Spanning Tree.
  - *Boundary*—The port on this instance is a boundary port. It inherits its state from instance 0 and can be viewed on the STP Interface Settings page.
- **Mode**—Displays the current interface Spanning Tree mode.
  - If the link partner is using MSTP or RSTP, the displayed port mode is RSTP.
  - If the link partner is using STP, the displayed port mode is STP.
- **Type**—Displays the MST type of the port.
  - *Boundary*—A Boundary port attaches MST bridges to a LAN in a remote region. If the port is a boundary port, it also indicates whether the device on the other side of the link is working in RSTP or STP mode.
  - *Internal*—The port is an internal port.
- **Designated Bridge ID**—Displays the ID number of the bridge that connects the link or shared LAN to the root.
- **Designated Port ID**—Displays the Port ID number on the designated bridge that connects the link or the shared LAN to the root.
- **Designated Cost**—Displays the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- **Remain Hops**—Displays the hops remaining to the next destination.
- **Forward Transitions**—Displays the number of times the port has changed from the Forwarding state to the Blocking state.

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

15

Managing MAC Address Tables

This section describe how to add MAC addresses to the system. It covers the following topics:

- **Configuring Static MAC Addresses**
- **Managing Dynamic MAC Addresses**
- **Defining Reserved MAC Addresses**

Types of MAC Addresses

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

Static addresses are configured by the user, and therefore, they do not expire.

A new source MAC address that appears in a frame arriving at the device is added to the Dynamic Address table. This MAC address is retained for a configurable period of time. If another frame with the same source MAC address does not arrive at the device before that time period expires, the MAC entry is aged (deleted) from the table.

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

The device supports a maximum of 8K static and dynamic MAC addresses.

Configuring Static MAC Addresses

Static MAC addresses are assigned to a specific physical interface and VLAN on the device. If that address is detected on another interface, it is ignored, and is not written to the address table.

To define a static address:

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

The Static Addresses page contains the currently defined static addresses.

STEP 2 Click **Add**.

STEP 3 Enter the parameters.

- **VLAN ID**—Select the VLAN ID for the port.
- **MAC Address**—Enter the interface MAC address.
- **Interface**—Select an interface (port, or LAG) for the entry.
- **Status**—Select how the entry is treated. The options are:
  - *Permanent*—The system never removes this MAC address. If the static MAC address is saved in the Startup Configuration, it is retained after rebooting.
  - *Delete on reset*—The static MAC address is deleted when the device is reset.
  - *Delete on timeout*—The MAC address is deleted when aging occurs.
  - *Secure*—The MAC address is secure when the interface is in classic locked mode (see **Configuring Port Security**).

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

Managing Dynamic MAC Addresses

The Dynamic Address Table (bridging table) contains the MAC addresses acquired by monitoring the source addresses of frames entering the device.

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

Configuring Dynamic MAC Address Aging Time

To configure the aging interval for dynamic addresses:

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

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

STEP 3 Click **Apply**. The aging time is updated.

Querying Dynamic Addresses

To query dynamic addresses:

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

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

- **VLAN ID**—Enter the VLAN ID for which the table is queried.
- **MAC Address**—Enter the MAC address for which the table is queried.
- **Interface**—Select the interface for which the table is queried. The query can search for specific unit/slot, ports, or LAGs.

STEP 3 Enter the **Dynamic Address Table Sort Key** field by which the table is sorted. The address table can be sorted by VLAN ID, MAC address, or interface.

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

To delete all of the dynamic MAC addresses. click **Clear Table**.

Defining Reserved MAC Addresses

When the device receives a frame with a Destination MAC address that belongs to a reserved range (per the IEEE standard), the frame can be discarded or bridged. The entry in the Reserved MAC Address Table can either specify the reserved MAC address or the reserved MAC address and a frame type:

To add an entry for a reserved MAC address:

STEP 1 Click **MAC Address Tables** > **Reserved MAC Addresses.** The Reserved MAC Addresses page opens.

STEP 2 Click **Add.**

STEP 3 Enter the values for the following fields:

- **MAC Address**—Select the MAC address to be reserved.
- **Frame Type**—Select a frame type based on the following criteria:
    - *Ethernet V2*—Applies to Ethernet V2 packets with the specific MAC address.
    - *LLC*—Applies to Logical Link Control (LLC) packets with the specific MAC address.
    - *LLC-SNAP*—Applies to Logical Link Control/Sub-Network Access Protocol (LLC-SNAP) packets with the specific MAC address.
    - *All*—Applies to all packets with the specific MAC address.
- **Action**—Select one of the following actions to be taken upon receiving a packet that matches the selected criteria:
    - *Discard*—Delete the packet.
    - *Bridge*—Forward the packet to all VLAN members.

Click **Apply.** A new MAC address is reserved.

16

Multicast

This section describes the Multicast Forwarding feature, and covers 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 device with Internet Group Membership Protocol (IGMP) snooping capabilities, or Multicast Listener Discovery (MLD) snooping, and a Multicast client that wants to receive a Multicast stream. In this setup, the router sends IGMP queries periodically.

NOTE MLD for IPv6 is derived from the IGMP v2 for IPv4. Even though the description in this section is mostly for IGMP, it also describes coverage of MLD where implied.

These queries reach the device, 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 device with the IGMP snooping analyzes the Join messages, and learns that the Multicast stream the host has requested must be forwarded to this specific port. It then forwards the IGMP Join to the Mrouter only. Similarly, when the Mrouter receives an IGMP Join message, it learns the interface from which it received the Join messages that wants to receive a specific Multicast stream. The Mrouter forwards the requested Multicast stream to the interface.

In a Layer 2 Multicast service, a Layer 2 switch receives a single frame addressed to a specific Multicast address. It creates copies of the frame to be transmitted on each relevant port.

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

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

When a device learns that a host is using IGMP/MLD messages to register to receive a Multicast stream, optionally from a specific source, the device adds the registration to its Multicast Forwarding Data Base (MFDB).

IGMP/MLD snooping can effectively reduce Multicast traffic from streaming bandwidth-intensive IP applications. A device using IGMP/MLD snooping only forwards Multicast traffic to the hosts interested in that traffic. This reduction of Multicast traffic reduces the packet processing at the device, and also reduces the workload of the end hosts, since they do not have to receive and filter all of the Multicast traffic generated in the network.

The following versions are supported:

- IGMP v1/v2/ v3
- MLD v1/v2
- A simple IGMP Snooping Querier

An IGMP Querier is required to facilitate the IGMP protocol on a given subnet. In general, a Multicast router is also an IGMP Querier. When there are multiple IGMP Queriers in a subnet, the queriers elect a single querier as the primary querier.

The device can be configured to be an IGMP Querier as a backup querier, or in situation where a regular IGMP Querier does not exist. The device is not a full capability IGMP Querier.

If the device is enabled as an IGMP Querier, it starts after 60 seconds have passed with no IGMP traffic (queries) detected from a Multicast router. In the presence of other IGMP Queriers, the device might (or might not) stop sending queries, based on the results of the standard querier selection process.

Multicast Address Properties

Multicast addresses have the following properties:

- Each IPv4 Multicast address is in the address range 224.0.0.0 to 239.255.255.255.
- The IPv6 Multicast address is FF00:/8.
- To map an IP Multicast group address to an Layer 2 Multicast address:
    - For IPv4, this is mapped by taking the 23 low-order bits from the IPv4 address, and adding them to the 01:00:5e prefix. By standard, the upper nine bits of the IP address are ignored, and any IP addresses that only differ in the value of these upper bits are mapped to the same Layer 2 address, since the lower 23 bits that are used are identical. For example, 234.129.2.3 is mapped to a MAC Multicast group address 01:00:5e:01:02:03. Up to 32 IP Multicast group addresses can be mapped to the same Layer 2 address.
    - For IPv6, this is mapped by taking the 32 low-order bits of the Multicast address, and adding the prefix of 33:33. For example, the IPv6 Multicast address FF00:1122:3344 is mapped to Layer 2 Multicast 33:33:11:22:33:44.

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 saved 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 device 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**.

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 device 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**.

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 contains 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.

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 saved to the Running Configuration file.

To configure and display the registration for the interfaces within the group, select an address, and click **Details.**

The page contains:

- **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 page contains all of the IP Multicast group addresses learned by snooping.

STEP 2 Enter the parameters required for filtering.

- **VLAN ID equals to**—Define the VLAN ID of the group to be displayed.
- **IP Version equals to**—Select IPv6 or IPv4.
- **IP Multicast Group Address equals to**—Define the IP address of the Multicast group to be displayed. This is only relevant when the Forwarding mode is (S,G).
- **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 the device in Layer 2 system mode, the IP Multicast address of Bonjour appears. Click **Go**. The results are displayed in the lower block.

STEP 4 Click **Add** to add a static IP Multicast Group Address.

STEP 5 Enter the parameters.

- **VLAN ID**—Defines the VLAN ID of the group to be added.
- **IP Version**—Select the IP address type.
- **IP Multicast Group Address**—Define the IP address of the new Multicast group.
- **Source 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.

- **Source IP 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 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).

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

NOTE The device 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.

The IGMP Snooping Querier is used to support a Layer 2 Multicast domain of snooping switches in the absence of a Multicast router. For example, where Multicast content is provided by a local server, but the router (if one exists) on that network does not support Multicast.

The speed of IGMP Querier activity must be aligned with the IGMP-snooping-enabled switches. Queries must be sent at a rate that is aligned to the snooping table aging time. If queries are sent at a rate lower than the aging time, the subscriber cannot receive the Multicast packets. This is performed in the IGMP Snooping Edit page.

To enable IGMP Snooping and identify the device as an IGMP Snooping Querier on a VLAN:

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

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 device only performs IGMP Snooping if both IGMP snooping and Bridge Multicast filtering are enabled.

STEP 3 Select a VLAN, and click **Edit**.

There can be only one IGMP Querier in a network. The device supports standards-based IGMP Querier election. Some of the values of the operational parameters of this table are sent by the elected querier. The other values are derived from the device.

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 device 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 device 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 device assumes there are no more members for the group, if the device 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 device 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.
- **IGMP Querier Status—**Enable or disable the IGMP Querier.
- **Administrative Querier Source IP Address—**Select the source IP address of the IGMP Querier. This can be the IP address of the VLAN or it can be the management IP address.
- **Operational Querier Source IP Address—**Displays the source IP address of the elected querier.
- **IGMP Querier Version—**Select the IGMP version used if the device becomes the elected querier. Select IGMPv3 if there are switches and/or Multicast routers in the VLAN that perform source-specific IP Multicast forwarding.

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

MLD Snooping

Hosts use the MLD protocol to report their participation in Multicast sessions, and the device uses MLD snooping to build Multicast membership lists. It uses these lists to forward Multicast packets only to device ports where there are host nodes that are members of the Multicast groups. The device does not support MLD Querier.

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

The device 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 device from stations to an upstream Multicast router and vice versa. This facility enables a device 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 and configure it on a VLAN:

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

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 device performs MLD Snooping only if both MLD snooping and Bridge Multicast filtering are enabled.

STEP 3 Select a VLAN, and click **Edit**.

STEP 4 Enter the parameters.

- **VLAN ID—**Select the VLAN ID.
- **MLD Snooping Status—**Enable or disable MLD snooping on the VLAN. The device monitors network traffic to determine which hosts have asked to be sent Multicast traffic. The device performs MLD snooping only when MLD snooping and Bridge Multicast filtering are both enabled
- **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 device 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 device if the device 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 device 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 device 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 device 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 device 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**.

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 device 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 device includes the Multicast router port(s) numbers 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**.

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 Forbidden is enabled on a port, Mrouter is not learned on this port (i.e. MRouter Ports Auto-Learn is not enabled on this port).
- None—The port is not currently a Multicast router port.

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

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 device.

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**.

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 device 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 device 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 device (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**.

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.

17

IP Configuration

IP interface addresses can be configured manually by the user, or automatically configured by a DHCP server. This section provides information for defining the device IP addresses, either manually or by making the device a DHCP client.

This section covers the following topics:

- **Overview**
- **IPv4 Management and Interfaces**
- **DHCP Server<300-500>**
- **IPv6 Management and Interfaces**
- **Domain Name**

Overview

Some features are only available in Layer 2 or Layer 3 system mode, as described below:

- In Layer 2 system mode, the device operates as a Layer 2 VLAN-aware device, and has no routing capabilities.
- In Layer 3 system mode, the device has IP routing capabilities as well as Layer 2 system mode capabilities. In this system mode, a Layer 3 port still retains much of the Layer 2 functionality, such as Spanning Tree Protocol and VLAN membership.

  In Layer 3 system mode, the device does not support MAC-based VLAN, Dynamic VLAN Assignment, VLAN Rate Limit, SYN Rate DoS Protection, and Advanced QoS Policers.

Configuring the device to work in either mode is performed in the Administration > System Settings page.

NOTE Switching from one system mode (layer) to another (on Sx500 devices) requires a mandatory reboot, and the startup configuration of the device is then deleted.

Layer 2 IP Addressing

In Layer 2 system mode, the device has up to one IPv4 address and up to two IPv6 interfaces (either “native” interface or Tunnel) 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 for Layer 2 system mode are configured on the IPv4 Interface and IPv6 Interfaces pages. In Layer 2 system mode, the device uses the default gateway, if configured, to communicate with devices that are not in the same IP subnet with the device. By default, VLAN 1 is the management VLAN, but this can be modified. When operating in Layer 2 system mode, the device can only be reached at the configured IP address through its management VLAN.

The factory default setting of the IPv4 address configuration is *DHCPv4*. This means that the device acts as a DHCPv4 client, and sends out a DHCPv4 request during boot up.

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

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

IP address collisions occur when the same IP address is used in the same IP subnet by more than one device. Address collisions require administrative actions on the DHCP server and/or the devices that collide with the device.

When a VLAN is configured to use dynamic IPv4 addresses, the device issues DHCPv4 requests until it is assigned an IPv4 address from a DHCPv4 server. In Layer 2 system mode, only the management VLAN can be configured with a static or dynamic IP address. In Layer 3 system mode, all the interface types (ports, LAGs, and/or VLANs) on the device can be configured with a static or dynamic IP address.

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

- When in Layer 2 system mode, unless the device is configured with a static IP address, it issues DHCPv4 requests until a response is received from the DHCP server.

- If the IP address on the device is changed, the device issues gratuitous ARP packets to the corresponding VLAN to check IP address collisions. This rule also applies when the device 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 device is acquiring an IP address and is currently using the factory default IP address 192.168.1.254.
- The same rules apply when a client must renew the lease, prior to its expiration date through a DHCPREQUEST message.
- With factory default settings, when no statically-defined or DHCP-acquired IP address is available, the default IP address is used. When the other IP addresses become available, the addresses are automatically used. The default IP address is always on the management VLAN.

Layer 3 IP Addressing

In Layer 3 system mode, the device can have multiple IP addresses. Each IP address can be assigned to specified ports, LAGs, or VLANs. These IP addresses are configured in the IPv4 Interface and IPv6 Interfaces pages in Layer 3 system mode. This provides more network flexibility than the Layer 2 system mode, in which only a single IP address can be configured. Operating in Layer 3 system mode, the device can be reached at all its IP addresses from the corresponding interfaces.

A predefined, default route is not provided in Layer 3 system mode. To remotely manage the device, a default route must be defined. All DHCP-assigned default gateways are stored as default routes. In addition, you can manually define default routes. This is defined in the IPv4 Static Routes and IPv6 Routes pages.

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

If the pages for Layer 2 and Layer 3 are different, both versions are displayed.

Loopback Interface

Overview

The loopback interface is a virtual interface whose operational state is always up. If the IP address that is configured on this virtual interface is used as the local address when communicating with remote IP applications, the communication will not be aborted even if the actual route to the remote application was changed.

The operational state of a loopback interface is always up. You define an IP address (either IPv4 or IPv6) on it and use this IP address as the local IP address for IP communication with remote IP applications.

A loopback interface does not support bridging; it cannot be a member of any VLAN, and no layer 2 protocol can be enabled on it.

The IPv6 link-local interface identifier is 1.

When the switch is in Layer 2 system mode, the following rules are supported:

- Only one loopback interface is supported.
- Two IPv4 interfaces can be configured: one on a VLAN or Ethernet port and one on the loopback interface.
- If the IPv4 address was configured on the default VLAN and the default VLAN is changed, the switch moves the IPv4 address to the new default VLAN.

Configuring a Loopback Interface

To configure an IPv4 loopback interface, do the following:

- In Layer 2, enable Loopback Interface and configure its address in Administration > Management Interface > IPv4 Interface page.
- In Layer 3, add a loopback interface in IP Configuration > IPv4 Management and Interfaces > IPv4 Interface.

To configure an IPv6 loopback interface, do the following:

- In Layer 2, add a loopback interface in the Administration > Management Interface > IPv6 Interfaces page. Configure the IPv6 address of that interface in the Administration > Management Interface > IPv6 Addresses page. This page is not available in SG500X, ESW2-550X and SG500XG devices.

- In Layer 3, add a loopback interface in IP Configuration > IPv6 Management and Interfaces > IPv6 Interface. Configure the IPv6 address of that interface in the IP Configuration > IPv6 Management and Interfaces > IPv6 Addresses page.

IPv4 Management and Interfaces

IPv4 Interface

IPv4 interfaces can be defined on the device when it is in Layer 2 or Layer 3 system mode.

Defining an IPv4 Interface in Layer 2 System Mode

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

To configure the IPv4 device IP address:

STEP 1 Click **Administration > Management Interface > IPv4 Interface**.

STEP 2 Enter values for the following fields:

- **Management VLAN**—Select the Management VLAN used to access the device 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.

NOTE DHCP Option 12 (Host Name option) is supported when the device is a DHCP client. If DHCP Option 12 is received from a DHCP server, it is saved as the server's host name. DHCP option 12 will not be requested by the device. The DHCP server must be configured to send option 12, regardless of what is requested in order to make use of this feature.

To configure a static IP address, configure the following fields.

- **IP Address—**Enter the IP address, and configure one of the following **Mask** fields:
  - **Network Mask—**Select and enter the IP address mask.
  - **Prefix Length—**Select and enter the length of the IPv4 address prefix.
- **Loopback Interface—**Select to enable the configuration of a loopback interface (see **Loopback Interface**).
- **Loopback IP Address—**Enter the IPv4 address of the loopback interface.

  Enter one of the following fields for the loopback interface:
  - *Loopback Mask*—Enter the mask of the IPv4 address of the loopback interface.
  - *Prefix Length*—Enter the prefix length of the IPv4 address of the loopback interface.
- **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 device 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 device dynamic IP address can be renewed any time after it is assigned by a DHCP server. Note that depending on your DHCP server configuration, the device might receive a new IP address after the renewal that requires setting the web-based configuration utility to the new IP address.
- **Auto Configuration via DHCP—**Displays status of Auto Configuration feature. You can configure this from *Administration* > *File Management* > *DHCP Auto Configuration*.

STEP 3 Click **Apply**. The IPv4 interface settings are written to the Running Configuration file.

Defining IPv4 Interface in Layer 3 System Mode

The IPv4 Interface page is used when the device is in Layer 3 system mode. This mode enables configuring multiple IP addresses for device management, and provides routing services.

The IP address can be configured on a port, a LAG, VLAN or loopback interface.

Operating in Layer 3 mode, the device routes traffic between the directly-attached IP subnets configured on the device. The device continues to bridge traffic between devices in the same VLAN. Additional IPv4 routes for routing to non-directly attached subnets can be configured in the IPv4 Static Routes page.

> **NOTE** The device software consumes one VLAN ID (VID) for every IP address configured on a port or LAG. The device takes the first VID that is not used starting from 4094.

To configure the IPv4 addresses:

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **IPv4 Interface.**

This page displays the following fields in the IPv4 Interface Table:

- **Interface**—Interface for which the IP address is defined.
- **IP Address Type**—IP address defined as static or DHCP.
    - *Dynamic IP Address*—Received from DHCP server.
    - *Static*—Entered manually.
- **IP Address**—Configured IP address for the interface.
- **Mask**—Configured IP address mask.
- **Status**—Results of the IP address duplication check.
    - *Tentative*—There is no final result for the IP address duplication check.
    - *Valid*—The IP address collision check was completed, and no IP address collision was detected.
    - *Valid-Duplicated*—The IP address duplication check was completed, and a duplicate IP address was detected.
    - *Duplicated*—A duplicated IP address was detected for the default IP address.

  - *Delayed*—The assignment of the IP address is delayed for 60 second if DHCP Client is enabled on startup in order to give time to discover DHCP address.
  - *Not Received*—Relevant for DHCP Address. When a DCHP Client starts a discovery process, it assigns a dummy IP address 0.0.0.0 before the real address is obtained. This dummy address has the status of “Not Received”.

STEP 2 Click **Add.**

STEP 3 Select one of the following fields:

- **Interface**—Select Port, LAG, or VLAN as the interface associated with this IP configuration, and select an interface from the list.
- **IP Address Type**—Select one of the following options:
  - *Dynamic IP Address*—Receive the IP address from a DHCP server.
  - *Static IP Address*—Enter the IP address.

STEP 4 Select**Dynamic Address or Static Address**.

STEP 5 If **Static Address** was selected, enter the IP Address for this interface, and enter one of the following:

- **Network Mask**—IP mask for this address.
- **Prefix Length**—Length of the IPv4 prefix.

STEP 6 Click **Apply**. The IPv4 address settings are written to the Running Configuration file.

IPv4 Routes

When the device is in Layer 3 system mode, this page enables configuring and viewing IPv4 static routes on the device. When routing traffic, the next hop is decided on according to the longest prefix match (LPM algorithm). A destination IPv4 address may match multiple routes in the IPv4 Static Route Table. The device uses the matched route with the highest subnet mask, that is, the longest prefix match.

To define an IP static route:

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **IPv4 Routes**.

STEP 2 Click **Add.**

STEP 3 Enter values for the following fields:

- **Destination IP Prefix—**Enter the destination IP address prefix.
- **Mask—**Select and enter information for one of the following:
  - **Network Mask—**The IP route prefix for the destination IP.
  - **Prefix Length—**The IP route prefix for the destination IP.
- **Route Type—**Select the route type.
  - *Reject*—Rejects the route and stops routing to the destination network via all gateways. This ensures that if a frame arrives with the destination IP of this route, it is dropped.
  - *Remote*—Indicates that the route is a remote path.
- **Next Hop Router IP Address—**Enter the next hop IP address or IP alias on the route.

  NOTE You cannot configure a static route through a directly-connected IP subnet where the device gets its IP address from a DHCP server.
- **Metric—**Enter the administrative distance to the next hop. The range is 1–255.

STEP 4 Click **Apply**. The IP Static route is saved to the Running Configuration file.

ARP

The device maintains an ARP (Address Resolution Protocol) table for all known devices that reside in the IP subnets directly connected to it. A directly-connected IP subnet is the subnet to which an IPv4 interface of the device is connected. When the device is required 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 device creates dynamic addresses from the ARP packets it receives. Dynamic addresses age out after a configured time.

NOTE In Layer 2 mode, the IP, MAC address mapping in ARP Table is used by the device to forward traffic originated by the device. In Layer 3 mode, the mapping information is used for Layer 3 routing as well as to forward generated traffic.

To define the ARP tables:

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **ARP**.

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 written to the Running Configuration file.

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**.

STEP 5 Enter the parameters:

- **IP Version**—The IP address format supported by the host. Only IPv4 is supported.
- **VLAN**—In Layer 2, displays the management VLAN ID.

For devices in Layer 2 mode, 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.

Interface—For devices in Layer 3 system mode, an IPv4 interface can be configured on a port, LAG or VLAN. Select the desired interface from the list of configured IPv4 interfaces on the device.

- **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 saved to the Running Configuration file.

ARP Proxy

The Proxy ARP technique is used by the device on a given IP subnet to answer ARP queries for a network address that is not on that network.

NOTE The ARP proxy feature is only available when the device is in L3 mode.

The ARP Proxy is aware of the destination of traffic, and offers another MAC address in reply. Serving as an ARP Proxy for another host effectively directs LAN traffic destination to the host. The captured traffic is then typically routed by the Proxy to the intended destination by using another interface, or by using a tunnel.

The process in which an ARP-query-request for a different IP address, for proxy purposes, results in the node responding with its own MAC address is sometimes referred to as publishing.

To enable ARP Proxy on all IP interfaces:

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **ARP Proxy**.

STEP 2 Select **ARP Proxy** to enable the device to respond to ARP requests for remotely-located nodes with the device MAC address.

STEP 3 Click **Apply**. The ARP proxy is enabled, and the Running Configuration file is updated.

UDP Relay/IP Helper

The UDP Relay/IP Helper feature is only available when the device is in Layer 3 system mode. Switches do not typically route IP Broadcast packets between IP subnets. However, if this feature enables the device to relay specific UDP Broadcast packets, received from its IPv4 interfaces, to specific destination IP addresses.

To configure the relaying of UDP packets received from a specific IPv4 interface with a specific destination UDP port, add a UDP Relay:

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **UDP Relay/IP Helper**.

STEP 2 Click **Add.**

STEP 3 Select the **Source IP Interface** to where the device is to relay UDP Broadcast packets based on a configured UDP destination port. The interface must be one of the IPv4 interfaces configured on the device.

STEP 4 Enter the **UDP Destination Port** number for the packets that the device is to relay. Select a well-known port from the drop-down list, or click the port radio button to enter the number manually.

STEP 5 Enter the **Destination IP Address** that receives the UDP packet relays. If this field is 0.0.0.0, UDP packets are discarded. If this field is 255.255.255.255, UDP packets are flooded to all IP interfaces.

STEP 6 Click **Apply**. The UDP relay settings are written to the Running Configuration file.

DHCPv4 Snooping/Relay

DHCPv4 Snooping

DHCP snooping provides a security mechanism to prevent receiving false DHCP response packets and to log DHCP addresses. It does this by treating ports on the device as either trusted or untrusted.

A trusted port is a port that is connected to a DHCP server and is allowed to assign DHCP addresses. DHCP messages received on trusted ports are allowed to pass through the device.

An untrusted port is a port that is not allowed to assign DHCP addresses. By default, all ports are considered untrusted until you declare them trusted (in the DHCP Snooping Interface Settings page).

DHCPv4 Relay

DHCP Relay relays DHCP packets to the DHCP server.

DHCPv4 in Layer 2 and Layer 3

In Layer 2 system mode, the device relays DHCP messages received from VLANs on which DHCP Relay has been enabled.

In Layer 3 system mode, the device can also relay DHCP messages received from VLANs that do not have IP addresses. Whenever DHCP Relay is enabled on a VLAN without an IP address, Option 82 is inserted automatically. This insertion is in the specific VLAN and does not influence the global administration state of Option 82 insertion.

Transparent DHCP Relay

For Transparent DHCP Relay where an external DHCP relay agent is being used, do the following:

- Enable DHCP Snooping.
- Enable Option 82 insertion.
- Disable DHCP Relay.

For regular DHCP Relay:

- Enable DHCP Relay.
- No need to enable Option 82 insertion.

Option 82

Option 82 (DHCP Relay Agent Information Option) passes port and agent information to a central DHCP server, indicating where an assigned IP address physically connects to the network.

The main goal of option 82 is to help to the DHCP server select the best IP subnet (network pool) from which to obtain an IP address.

The following Option 82 options are available on the device:

- **DHCP Insertion -** Add Option 82 information to packets that do not have foreign Option 82 information.
- **DHCP Passthrough -** Forward or reject DHCP packets that contain Option 82 information from untrusted ports. On trusted ports, DHCP packets containing Option 82 information are always forwarded.

The following table shows the packet flow through the DHCP Relay, DHCP Snooping, and Option 82 modules:

The following cases are possible:

- DHCP client and DHCP server are connected to the same VLAN. In this case, a regular bridging passes the DHCP messages between DHCP client and DHCP server.
- DHCP client and DHCP server are connected to different VLANs. In the case, only DHCP Relay can and does broadcast DHCP messages between DHCP client and DHCP server. Unicast DHCP messages are passed by regular routers and therefore if DHCP Relay is enabled on a VLAN without an IP address or if the device is not a router (Layer 2 device) then an external router is needed.

DHCP Relay and only DHCP Relay relays DHCP messages to a DHCP server

Interactions Between DHCPv4 Snooping, DHCPv4 Relay and Option 82

The following tables describe how the device behaves with various combinations of DHCP Snooping, DHCP Relay and Option 82.

The following describes how DHCP request packets are handled when DHCP Snooping is not enabled and DHCP Relay is enabled.

	DHCP Relay **VLAN with IP Address**		**DHCP Relay** **VLAN without IP Address**	
	Packet arrives without Option 82	Packet arrives with Option 82	Packet arrives without Option 82	Packet arrives with Option 82

	DHCP Relay **VLAN with IP Address**		**DHCP Relay** **VLAN without IP Address**	
Option 82 Insertion Disabled	Packet is sent without Option 82	Packet is sent with the original Option 82	Relay – inserts Option 82 Bridge – no Option 82 is inserted	Relay – discards the packet Bridge – Packet is sent with the original Option 82
Option 82 Insertion Enabled	Relay – is sent with Option 82 Bridge – no Option 82 is sent	Packet is sent with the original Option 82	Relay – is sent with Option 82 Bridge – no Option 82 is sent	Relay – discards the packet Bridge – Packet is sent with the original Option 82

The following describes how DHCP request packets are handled when both DHCP Snooping and DHCP Relay are enabled:

	DHCP Relay **VLAN with IP Address**		**DHCP Relay** **VLAN without IP Address**	
	Packet arrives without Option 82	Packet arrives with Option 82	Packet arrives without Option 82	Packet arrives with Option 82
Option 82 Insertion Disabled	Packet is sent without Option 82	Packet is sent with the original Option 82	Relay – inserts Option 82 Bridge – no Option 82 is inserted	Relay – discards the packet Bridge – Packet is sent with the original Option 82

	DHCP Relay VLAN with IP Address		DHCP Relay VLAN without IP Address	
Option 82 Insertion Enabled	Relay – is sent with Option 82 Bridge – Option 82 is added (if port is trusted, behaves as if DHCP Snooping is not enabled)	Packet is sent with the original Option 82	Relay – is sent with Option 82 Bridge – Option 82 is inserted (if port is trusted, behaves as if DHCP Snooping is not enabled)	Relay – discards the packet Bridge – Packet is sent with the original Option 82

The following describes how DHCP Reply packets are handled when DHCP Snooping is disabled:

	DHCP Relay VLAN with IP Address		DHCP Relay VLAN without IP Address	
	Packet arrives without Option 82	Packet arrives with Option 82	Packet arrives without Option 82	Packet arrives with Option 82

	DHCP Relay **VLAN with IP Address**		**DHCP Relay** **VLAN without IP Address**	
Option 82 insertion disabled	Packet is sent without Option 82	Packet is sent with the original Option 82	Relay – discards Option 82 Bridge – Packet is sent without Option 82	Relay – 1. If reply originates in device, packet is sent without Option 82 2. If reply does not originate in device, packet is discarded Bridge – Packet is sent with the original Option 82
Option 82 insertion enabled	Packet is sent without Option 82	Relay – Packet is sent without Option 82 Bridge – Packet is sent with the Option 82	Relay – discards Option 82 Bridge – Packet is sent without Option 82	Relay – Packet is sent without Option 82 Bridge – Packet is sent with the Option 82

The following describes how DHCP reply packets are handled when both DHCP Snooping and DHCP Relay are enabled

	DHCP Relay VLAN with IP Address		DHCP Relay VLAN without IP Address	
	Packet arrives without Option 82	Packet arrives with Option 82	Packet arrives without Option 82	Packet arrives with Option 82
Option 82 Insertion Disabled	Packet is sent without Option 82	Packet is sent with the original Option 82	Relay discards Option 82 Bridge - Packet is sent without Option 82	Relay 1. If reply originates on the device, packet is sent without Option 82 2. If reply does not originate on the device, discards the packet Bridge – Packet is sent with the original Option 82
Option 82 Insertion Enabled	Packet is sent without Option 82	Packet is sent without Option 82	Relay – discards Option 82 Bridge – Packet is sent without Option 82	Packet is sent without Option 82

DHCP Snooping Binding Database

DHCP Snooping builds a database (known as the DHCP Snooping Binding database) derived from information taken from DHCP packets entering the device through trusted ports.

The DHCP Snooping Binding database contains the following data: input port, input VLAN, MAC address of the client and IP address of the client if it exists.

The DHCP Snooping Binding database is also used by IP Source Guard and Dynamic ARP Inspection features to determine legitimate packet sources.

DHCP Trusted Ports

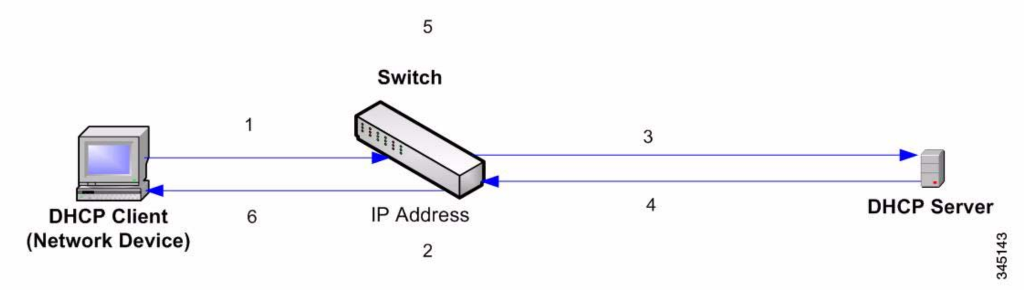
Ports can be either DHCP trusted or untrusted. By default, all ports are untrusted. To create a port as trusted, use the DHCP Snooping Interface Settings page. Packets from these ports are automatically forwarded. Packets from trusted ports are used to create the Binding database and are handled as described below.

If DHCP Snooping is not enabled, all ports are trusted by default.

How the DHCP Snooping Binding Database is Built

The following describes how the device handles DHCP packets when both the DHCP client and DHCP server are trusted. The DHCP Snooping Binding database is built in this process.

DHCP Trusted Packet Handling



The actions are:

STEP 1 Device sends DHCPDISCOVER to request an IP address or DHCPREQUEST to accept an IP address and lease.

STEP 2 Device snoops packet and adds the IP-MAC information to the DHCP Snooping Binding database.

STEP 3 Device forwards DHCPDISCOVER or DHCPREQUEST packets.

STEP 4 DHCP server sends DHCPOFFER packet to offer an IP address, DHCPACK to assign one, or DHCPNAK to deny the address request.

STEP 5 Device snoops packet. If an entry exists in the DHCP Snooping Binding table that matches the packet, the device replaces it with IP-MAC binding on receipt of DHCPACK.

STEP 6 Device forwards DHCPOFFER, DHCPACK, or DHCPNAK.

The following summarizes how DHCP packets are handled from both trusted and untrusted ports. The DHCP Snooping Binding database is stored in non-volatile memory.

DHCP Snooping Packet Handling

Packet Type	Arriving from Untrusted Ingress Interface	Arriving from Trusted Ingress Interface
DHCPDISCOVER	Forward to trusted interfaces only.	Forwarded to trusted interfaces only.
DHCPOFFER	Filter.	Forward the packet according to DHCP information. If the destination address is unknown the packet is filtered.
DHCPREQUEST	Forward to trusted interfaces only.	Forward to trusted interfaces only.
DHCPACK	Filter.	Same as DHCPOFFER and an entry is added to the DHCP Snooping Binding database.
DHCPNAK	Filter.	Same as DHCPOFFER. Remove entry if exists.
DHCPDECLINE	Check if there is information in the database. If the information exists and does not match the interface on which the message was received, the packet is filtered. Otherwise the packet is forwarded to trusted interfaces only, and the entry is removed from database.	Forward to trusted interfaces only

Packet Type	Arriving from Untrusted Ingress Interface	Arriving from Trusted Ingress Interface
DHCPRELEASE	Same as DHCPDECLINE.	Same as DHCPDECLINE.
DHCPINFORM	Forward to trusted interfaces only.	Forward to trusted interfaces only.
DHCPLEASEQUERY	Filtered.	Forward.

DHCP Snooping Along With DHCP Relay

If both DHCP Snooping and DHCP Relay are globally enabled, then if DHCP Snooping is enabled on the client's VLAN, DHCP Snooping rules contained in the DHCP Snooping Binding database are applied, and the DHCP Snooping Binding database is updated in the client's and DHCP server’s VLAN, for packets that are relayed.

DHCP Default Configuration

The following describes DHCP Snooping and DHCP Relay default options.

DHCP Default Options

Option	Default State
DHCP Snooping	**Enabled**
Option 82 Insertion	**Not enabled**
Option 82 Passthrough	**Not enabled**
Verify MAC Address	**Enabled**
Backup DHCP Snooping Binding Database	**Not enabled**
DHCP Relay	**Disabled**

Configuring DHCP Work Flow

To configure DHCP Relay and DHCP Snooping:

STEP 1 Enable DHCP Snooping and/or DHCP Relay in the **IP Configuration > DHCP > Properties** page or in the **Security > DHCP Snooping > Properties** page.

STEP 2 Define the interfaces on which DHCP Snooping is enabled in the **IP Configuration > DHCP > Interface Settings** page.

STEP 3 Configure interfaces as trusted or untrusted in the **IP Configuration > DHCP > DHCP Snooping Interface** page.

STEP 4 Optional. Add entries to the DHCP Snooping Binding database in the **IP Configuration > DHCP > DHCP Snooping Binding Database** page.

DHCP Snooping/Relay

This section describes how the DHCP Relay and Snooping features are implemented via the Web-based interface.

Properties

To configure DHCP Relay, DHCP Snooping and Option 82:

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Snooping/Relay** > **Properties** or **Security** > **DHCP Snooping.**

Enter the following fields:

- **Option 82—**Select **Option 82** to insert Option 82 information into packets.
- **DHCP Relay—**Select to enable DHCP Relay.
- **DHCP Snooping Status—**Select to enable DHCP Snooping. If DHCP Snooping is enabled, the following options can be enabled:
  - *Option 82 Passthrough*—Select to leave foreign Option 82 information when forwarding packets.
  - *Verify MAC Address*—Select to verify that the source MAC address of the Layer 2 header matches the client hardware address as appears in the DHCP Header (part of the payload) on DHCP untrusted ports.
  - *Backup Database*—Select to back up the DHCP Snooping Binding database on the device's flash memory.
  - *Backup Database Update Interval*—Enter how often the DHCP Snooping Binding database is to be backed up **(if Backup Database is selected).**

STEP 2 Click **Apply**. The settings are written to the Running Configuration file.

STEP 3 To define a DHCP server, click **Add**.

STEP 4 Enter the IP address of the DHCP server and click **Apply**. The settings are written to the Running Configuration file.

Interface Settings

In Layer 2, DHCP Relay and Snooping can only be enabled on VLANs with IP addresses.

In Layer 3, DHCP Relay and Snooping can be enabled on any interface with an IP address and on VLANs with or without an IP address.

To enable DHCP Snooping/Relay on specific interfaces:

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Snooping/ Relay** > **Interface Settings**.

STEP 2 To enable DHCP Relay or DHCP Snooping on an interface, click **ADD**.

STEP 3 Select the interface and the features to be enabled: **DHCP Relay** or **DHCP Snooping**.

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

DHCP Snooping Trusted Interfaces

Packets from untrusted ports/LAGs are checked against the DHCP Snooping Binding database (see the DHCP Snooping Binding Database page).

By default, interfaces are trusted.

To designate an interface as untrusted:

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Snooping/ Relay** > **DHCP Snooping Trusted Interfaces**.

STEP 2 Select the interface and click **Edit**.

STEP 3 Select **Trusted Interface** (Yes or No).

STEP 4 Click **Apply** to save the settings to the Running Configuration file.

DHCP Snooping Binding Database

See **How the DHCP Snooping Binding Database is Built** for a description of how dynamic entries are added to the DHCP Snooping Binding database.

Note the following points about maintenance of the DHCP Snooping Binding database:

- The device does not update the DHCP Snooping Binding database when a station moves to another interface.
- If a port is down, the entries for that port are not deleted.
- When DHCP Snooping is disabled for a VLAN, the binding entries that were collected for that VLAN are removed.
- If the database is full, DHCP Snooping continue to forward packets but new entries are not created. Note that if the IP source guard and/or ARP inspection features are active, the clients that are not written in the DHCP Snooping Binding database are not be able to connect to the network.

To add entries to the DHCP Snooping Binding database:

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Snooping/ Relay** > **DHCP Snooping Binding Database**.

To see a subset of entries in the DHCP Snooping Binding database, enter the relevant search criteria and click **Go**.

The fields in the DHCP Snooping Binding Database are displayed. These are described in the Add page, except for the **IP Source Guard** field:

- **Status—**
    - Active—IP Source Guard is active on the device.
    - Inactive—IP Source Guard is not active on the device.
- **Reason—**
    - No Problem
    - No Resource
    - No Snoop VLAN
    - Trust Port

STEP 2 To add an entry, click **Add**.

STEP 3 Enter the fields:

- **VLAN ID**—VLAN on which packet is expected.
- **MAC Address**—MAC address of packet.
- **IP Address**—IP address of packet.
- **Interface**—Unit/Slot/Interface on which packet is expected.
- **Type**—The possible field values are:
    - *Dynamic*—Entry has limited lease time.
    - *Static*—Entry was statically configured.
- **Lease Time**—If the entry is dynamic, enter the amount of time that the entry is to be active in the DHCP Database. If there is no Lease Time, check Infinite.)

STEP 4 Click **Apply**. The settings are defined, and the device is updated.

DHCP Server

The DHCPv4 Server feature enables you to configure the device as a DHCPv4 server. A DHCPv4 server is used to assign IPv4 address and other information to another device (DHCP client)

The DHCPv4 server allocates IPv4 addresses from a user-defined pool of IPv4 addresses.

These can be in the following modes:

- **Static Allocation**—The hardware address or client identifier of a host is manually mapped to an IP address. This is done in the Static Hosts page.
- **Dynamic Allocation**—A client obtains a leased IP address for a specified period of time (that can be infinite). If the DHCP client does not renew the allocated IP Address, the IP address is revoked at the end of this period, and the client must request another IP address. This is done in the Network Pools page.

Dependencies Between Features

- It is impossible to configure DHCP server and DHCP client on the system at the same time, meaning: if one interface is DHCP client enabled, it is impossible to enable DHCP server globally.
- If DHCPv4 Relay is enabled, the device cannot be configured as a DHCP server.

Default Settings and Configurations

- The device is not configured as a DHCPv4 server by default.
- If the device is enabled to be a DHCPv4 server, there are no network pools of addresses defined by default.

Workflow for Enabling the DHCP Server Feature

To configure the device as a DHCPv4 server:

STEP 1 Enable the device as a DHCP server using the DHCP Server > Properties page.

STEP 2 If there are any IP addresses that you do not want to be assigned, configure them using the Excluded Addresses page.

STEP 3 Define up to 8 network pools of IP addresses using the Network Pools page.

STEP 4 Configure clients that will be assigned a permanent IP address, using the Static Hosts page.

STEP 5 Configure the required DHCP options in the DHCP Options page. This configures the values to be returned for every relevant DHCP option.

STEP 6 Add an IP interface in the range of one of the configured DHCP pools in the Network Pools page. The device answers DHCP queries from this IP interface. For example: if the pool's range is 1.1.1.1 -1.1.1.254, add an IP address in this range, if you want directly-connected clients to receive IP address from the configured pool. Do this in the IP Configuration > IPv4 Interface page.

STEP 7 View the allocated IP addresses using the Address Binding page. IP addresses can be deleted in this page.

DHCPv4 Server

To configure the device as a DHCPv4 server:

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Server** > **Properties** to display the Properties page.

STEP 2 Select **Enable** to configure the device as a DHCP server.

STEP 3 Click **Apply.** The device immediately begins functioning as a DHCP server. However, it does not assign IP addresses to clients until a pool is created.

Network Pool

When the device is serving as a DHCP server, one or more pools of IP addresses must be defined, from which the device will allocate IP addresses to clients. Each network pool contains a range of addresses that belong to a specific subnetwork. These addresses are allocated to various clients within that subnet.

When a client requests an IP address, the device as DHCP server allocates an IP address according to the following:

- **Directly-attached Client**—The device allocates an address from the network pool whose subnet matches the subnet configured on the device's IP interface from which the DHCP request was received.
- **Remote Client**—The devices takes an IP address from the network pool whose first relay subnet, which is connected directly to the client, matches the subnet configured on one of switches IP interfaces.

Up to eight network pools can be defined.

To create a pool of IP addresses, and define their lease durations:

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Server** > **Network Pool** to display the Network Pool page.

The previously-defined network pools are displayed.

STEP 2 Click **Add** to define a new network pool. Note that you either enter the Subnet IP Address and the Mask, or enter the Mask, the Address Pool Start and Address Pool End.

STEP 3 Enter the fields:

- **Pool Name—**Enter the pool name.
- **Subnet IP Address—**Enter the subnet in which the network pool resides.

- **Mask**—Enter one of following:
  - **Network Mask**—Check and enter the pool's network mask.
  - **Prefix Length**—Check and enter the number of bits that comprise the address prefix.
- **Address Pool Start—**Enter the first IP address in the range of the network pool.
- **Address Pool End—**Enter the last IP address in the range of the network pool.
- **Lease Duration**—Enter the amount of time a DHCP client can use an IP address from this pool. You can configure a lease duration of up to 49,710 days or an infinite duration.
  - **Infinite**—The duration of the lease is unlimited.
  - **Days**—The duration of the lease in number of days. The range is 0 to 49710 days.
  - **Hours**—The number of hours in the lease. A days value must be supplied before an hours value can be added.
  - **Minutes**—The number of minutes in the lease. A days value and an hours value must be added before a minutes value can be added.
- **Default Router IP Address (Option 3)**— Enter the default router for the DHCP client.
- **Domain Name Server IP Address (Option 6)**—Select one of the devices DNS servers (if already configured) or select **Other** and enter the IP address of the DNS server available to the DHCP client.
- **Domain Name (Option 15)**—Enter the domain name for a DHCP client.
- **NetBIOS WINS Server (Option 44)**— Enter the NetBIOS WINS name server available to a DHCP client.
- **NetBIOS Node Type (Option 46)**—Select how to resolve the NetBIOS name. Valid node types are:
  - *Hybrid*—A hybrid combination of b-node and p-node is used. When configured to use h-node, a computer always tries p-node first and uses b-node only if p-node fails. This is the default.

  - *Mixed*—A combination of b-node and p-node communications is used to register and resolve NetBIOS names. M-node first uses b-node; then, if necessary, p-node. M-node is typically not the best choice for larger networks because its preference for b-node Broadcasts increases network traffic.
  - *Peer-to-Peer*—Point-to-point communications with a NetBIOS name server are used to register and resolve computer names to IP addresses.
  - *Broadcast*—IP Broadcast messages are used to register and resolve NetBIOS names to IP addresses.
- **SNTP Server IP Address (Option 4)**— Select one of the device's SNTP servers (if already configured) or select **Other** and enter the IP address of the time server for the DHCP client.
- **File Server IP Address (siaddr)**—Enter the IP address of the TFTP/SCP server from which the configuration file is downloaded.
- **File Server Host Name (sname)**—Enter the name of the TFTP/SCP server.
- **Configuration File Name (file)**—Enter the name of the file that is used as a configuration file.

Excluded Addresses

By default, the DHCP server assumes that all pool addresses in a pool may be assigned to clients. A single IP address or a range of IP addresses can be excluded. The excluded addresses are excluded from all DHCP pools.

To define an excluded address range:

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Server** > **Excluded Addresses** to display the Excluded Addresses page.

The previously-defined excluded IP addresses are displayed.

STEP 2 To add a range of IP addresses to be excluded, click **Add**, and enter the fields:

- **Start IP Address**—First IP address in the range of excluded IP addresses.
- **End IP Address**—Last IP address in the range of excluded IP addresses.

Static Hosts

You might want to assign some DHCP clients a permanent IP address that never changes. This client is then known as a static host.

To manually allocate a permanent IP address to a specific client:

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Server** > **Static Hosts** to display the Static Hosts page.

The static hosts are displayed.

STEP 2 To add a static host, click **Add**, and enter the fields:

- **IP Address—**Enter the IP address that was statically assigned to the host.
- **Host Name—**Enter the host name, which can be a string of symbols and an integer.
- **Mask—**Enter the static host's network mask.
  - *Network Mask*—Check and enter the static host's network mask.
  - *Prefix Length*—Check and enter the number of bits that comprise the address prefix.
- **Identifier Type—**Set how to identify the specific static host.
  - *Client Identifier*—Enter a unique identification of the client specified in hexadecimal notation, such as: 01b60819681172.

or:

  - *MAC Address*—Enter the MAC address of the client.
- **Client Name—**Enter the name of the static host, using a standard set of ASCII characters. The client name must not include the domain name.
- **Default Router IP Address (Option 3)—** Enter the default router for the static host.
- **Domain Name Server IP Address (Option 6)—**Select one of the devices DNS servers (if already configured) or select **Other** and enter the IP address of the DNS server available to the DHCP client.
- **Domain Name (Option 15)—**Enter the domain name for the static host.
- **NetBIOS WINS Server (Option 44)—** Enter the NetBIOS WINS name server available to the static host.
- **NetBIOS Node Type (Option 46)—**Select how to resolve the NetBIOS name. Valid node types are:

  - *Hybrid*—A hybrid combination of b-node and p-node is used. When configured to use h-node, a computer always tries p-node first and uses b-node only if p-node fails. This is the default.
  - *Mixed*—A combination of b-node and p-node communications is used to register and resolve NetBIOS names. M-node first uses b-node; then, if necessary, p-node. M-node is typically not the best choice for larger networks because its preference for b-node Broadcasts increases network traffic.
  - *Peer-to-Peer*—Point-to-point communications with a NetBIOS name server are used to register and resolve computer names to IP addresses.
  - *Broadcast*—IP Broadcast messages are used to register and resolve NetBIOS names to IP addresses.
- **SNTP Server IP Address (Option 4)**— Select one of the device's SNTP servers (if already configured) or select **Other** and enter the IP address of the time server for the DHCP client.
- **File Server IP Address (siaddr)**—Enter the IP address of the TFTP/SCP server from which the configuration file is downloaded.
- **File Server Host Name (sname)**—Enter the name of the TFTP/SCP server.
- **Configuration File Name (file)**—Enter the name of the file that is used as a configuration file.

DHCP Options

When the device is acting as a DHCP server, the DHCP options can be configured using the HEX option. A description of these options can be found in RFC2131.

The configuration of these options determines the reply that is sent to DHCP clients whose packets include a request (using option 55) for the configured DHCP options.

The options that are configured specifically on the DHCP Server >Network Pools and the DHCP Server >Static Hosts pages (Option 3-6, 15, 44, 46, 66, 67) cannot be configured using the DHCP Options page.

Example: The DHCP option 66 is configured with the name of a TFTP server in the DHCP Options page. When a client DHCP packet is received containing option 66, the TFTP server is returned as the value of option 66.

To configure one or more DHCP options:

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Server** > **DHCP Options.**

The previously-configured DHCP options are displayed..

STEP 2 To configure an option that has not been configured yet and enter the field:

- **DHCP Server Pool Name—**Select one of the pool of network addresses defined in the Network Pools page.

STEP 3 Click **Add** and enter the fields:

- **Code—** Enter the DHCP option code.
- **Type—** The radio buttons for this field, change according to the type of the DHCP option's parameter. Select one of the following codes and enter the value for the DHCP options parameter:
  - *Hex*—Select if you want to enter the hex value of the parameter for the DHCP option. A hex value can be provided in place of any other type of value. For instance, you can provide a hex value of an IP address instead of the IP address itself.

    No validation is made of the hex value, therefore if you enter a HEX value, which represents an illegal value, no error is provided, and the client might not be able to handle the DHCP packet from the server.
  - *IP*—Select if you want to enter an IP address when this is relevant for the DHCP option selected.
  - *IP List*—Enter list of IP addresses separated by commas.
  - *Integer*—Select if you want to enter an integer value of the parameter for the DHCP option selected.
  - *Boolean*—Select if the parameter for the DHCP option selected is Boolean.
- **Boolean Value—** If the type was Boolean, select the value to be returned: **True** or **False**.
- **Value—** If the type is not Boolean, enter the value to be sent for this code.
- **Description—** Enter a text description for documentation purposes.

Address Binding

Use the Address Binding page to view and remove the IP addresses allocated by the device and their corresponding MAC addresses.

To view and/or remove address bindings:

STEP 1 Click **IP Configuration** > **IPv4 Management and Interfaces** > **DHCP Server** > **Address Binding** to display the Address Binding page.

The following fields for the address bindings are displayed:

- **IP Address**—The IP addresses of the DHCP clients.
- **Address Type**— Whether the address of the DHCP client appears as a MAC address or using a client identifier.
- **MAC Address/Client Identifier**—A unique identification of the client specified as a MAC Address or in hexadecimal notation, e.g., 01b60819681172.
- **Lease Expiration**—The lease expiration date and time of the host's IP address or Infinite is such was the lease duration defined.
- **Type**—The manner in which the IP address was assigned to the client. The possible options are:
    - *Static*—The hardware address of the host was mapped to an IP address.
    - *Dynamic*—The IP address, obtained dynamically from the device, is owned by the client for a specified period of time. The IP address is revoked at the end of this period, at which time the client must request another IP address.
- **State**—The possible options are:
    - *Allocated*—IP address has been allocated. When a static-host is configured, its state is allocated.
    - *Declined*—IP address was offered but not accepted, therefore it is not allocated.
    - *Expired*—The lease of the IP address has expired.
    - *Pre-Allocated*—An entry will be in pre-allocated state from the time between the offer and the time that the DHCP ACK is sent from the client. Then it becomes allocated.

IPv6 Management and Interfaces

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 either an ISATAP or manual mechanism (see **IPv6 Tunnel**). Tunneling treats the IPv4 network as a virtual IPv6 local link, with mappings from each IPv4 address to a link local IPv6 address.

The device detects IPv6 frames by the IPv6 Ethertype.

IPv6 Global Configuration

To define IPv6 global parameters and DHCPv6 client settings:

STEP 1 In Layer 2 system mode, click **Administration** > **Management Interface** > **IPv6 Global Configuration**.

In Layer 3 system mode, click **IP Configuration** > **IPv6 Management and Interfaces** > **IPv6 Global Configuration**.

STEP 2 Enter values for the following fields:

- **ICMPv6 Rate Limit Interval**—Enter how often the ICMP error messages are generated.
- **ICMPv6 Rate Limit Bucket Size**—Enter the maximum number of ICMP error messages that can be sent by the device per interval.

DHCPv6 Client Settings

- **Unique Identifier (DUID) Format—**This is the identifier of the DHCP client that is used by the DHCP server to locate the client. It can be in one of the following formats:
    - *Link-Layer*—(Default). If you select this option, the MAC address of the device is used.
    - *Enterprise Number*—If you select this option, enter the following fields.
- **Enterprise Number—**The vendors registered Private Enterprise number as maintained by IANA.
- **Identifier—**The vendor-defined hex string (up to 64 hex characters). If the number of the character is not even, a zero is added at the right. Each 2 hex characters can be separated by a period or colon.
- **DHCPv6 Unique Identifier (DUID)—**Displays the identifier selected.

IPv6 Interface

An IPv6 interface can be configured on a port, LAG, VLAN, loopback interface or tunnel.

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

To define an IPv6 interface:

STEP 1 In Layer 2 system mode, click **Administration** > **Management Interface** > **IPv6 Interfaces**.
In Layer 3 system mode, click **IP Configuration** > **IPv6 Management and Interfaces** > **IPv6 Interfaces**.

STEP 2 Click **Add** to add a new interface on which interface IPv6 is enabled.

STEP 3 Enter the fields:

- **IPv6 Interface—**Select a specific port, LAG, VLAN, or ISATAP tunnel for the IPv6 address.

STEP 4 To configure the interface as a DHCPv6 client, meaning to enable the interface to receive information from the DHCPv6 server, such as: SNTP configuration and DNS information, enter the **DHCPv6 Client** fields:

- **Stateless**—Select to enable the interface as a stateless DHCPv6 client. This enables reception of configuration information from a DHCP server.
- **Minimum Information Refresh Time**—This value is used to put a floor on the refresh time value. If the server sends a refresh time option that is less than this value, this value is used instead. Select either **Infinite** (no refresh unless the server sends this option) or **User Defined** to set a value.
- **Information Refresh Time**—This value indicates how often the device will refresh information received from the DHCPv6 server. If this option is not received from the server, the value entered here is used. Select either **Infinite** (no refresh unless the server sends this option) or **User Defined** to set a value.

STEP 5 To configure additional IPv6 parameters, enter the following fields:

- **IPv6 Address Auto Configuration**—Select to enable automatic address configuration from router advertisements sent by neighbors.

  NOTE The device does not support stateful address auto configuration from a DHCPv6 server.

- **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.
- **Send ICMPv6 Messages**—Enable generating unreachable destination messages.

STEP 6 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 7 Click **IPv6 Address Table** to manually assign IPv6 addresses to the interface, if required. This page is described in the **Defining IPv6 Addresses** section.

STEP 8 Press the **Restart** button to initiate refresh of the stateless information received from the DHCPv6 server.

DHCPv6 Client Details

The **DHCPv6 Client Details** button displays information received on the interface from a DHCPv6 server.

It is active when the interface selected is defined as a DHCPv6 stateless client.

When the button is pressed, it displays the following fields (for the information that was received from the DHCP server):

- **DHCPv6 Operational Mode**—This displays Enabled if the following conditions are fulfilled:
  - The interface is Up.
  - IPv6 is enabled on it.
  - DHCPv6 stateless client is enabled on it.
- **Stateless Service**—Is the client defined as stateless (receives configuration information from a DHCP server) or not.
- **DHCPv6 Server Address**—Address of DHCPv6 server.
- **DHCPv6 Server DUID**—Unique identifier of the DHCPv6 server.
- **DHCPv6 Server Preference**—Priority of this DHCPv6 server.
- **Information Minimum Refresh Time**— See above.
- **Information Refresh Time**—See above.
- **Received Information Refresh Time**—Refresh time received from DHCPv6 server.
- **Remaining Information Refresh Time**—Remaining time until next refresh.
- **DNS Servers**—List of DNS servers received from the DHCPv6 server.
- **DNS Domain Search List**—List of domains received from the DHCPv6 server.
- **SNTP Servers**—List of SNTP servers received from the DHCPv6 server.
- **POSIX Timezone String**—Timezone received from the DHCPv6 server.
- **Configuration Server**—Server containing configuration file received from the DHCPv6 server.

- **Configuration Path Name**—Path to configuration file on the configuration server received from the DHCPv6 server.

IPv6 Tunnel

Tunnels enable transmission of IPv6 packets over IPv4 networks. Each tunnel has a source IPv4 address and a destination IPv4 address. The IPv6 packet is encapsulated between these addresses.

ISATAP Tunnels

The type of tunnel that can be configured on the device is called an Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnel, which is a point-to-multi-point tunnel. The source address is the IPv4 address (or one of the IPv4 addresses) of the device.

When configuring an ISATAP tunnel, the destination IPv4 address is provided by the router. 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, the ISATAP host name-to-address mapping is searched for 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.

Configuring Tunnels

NOTE To configure a tunnel, first configure an IPv6 interface as a tunnel in the IPv6 Interfaces page.

To configure an IPv6 tunnel:

STEP 1 In Layer 2 system mode, click **Administration > Management Interface > IPv6 Tunnel**.

In Layer 3 system mode, click **IP Configuration > IPv6 Management and Interfaces > IPv6 Tunnel**.

STEP 2 Enter values for the following fields:

- **Tunnel Number**—Displays the automatic tunnel router domain number.
- **Tunnel Type**—Always ISATAP.
- **Source IPv4 Address**—The IPv4 address of the selected interface on the current device used to form part of the IPv6 address.
  - *Auto*—Automatically selects the lowest IPv4 address from among all of its configured IPv4 interfaces on the device. This option is equivalent to the Interface option in Layer 3, because in Layer 2 there is only one interface.

    NOTE If the IPv4 address is changed, the local address of the tunnel interface is also changed.
  - *None*—Disable the tunnel.
  - *Manual*—Enter the IPv4 source address to be used. The IPv4 address configured must be one of the IPv4 addresses of the devices IPv4 interfaces.
  - *Interface*—(In Layer 3) Select the IPv4 interface to be used.
- **ISATAP Router 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.
- **ISATAP Solicitation Interval**—The number of seconds between ISATAP router solicitations messages, when there is no active ISATAP router. The interval can be the default value or a user defined interval.
- **ISATAP Robustness**—Used to calculate the interval for the DNS or router solicitation queries. The larger the number, the more frequent the queries.

  NOTE The ISATAP tunnel is not operational if the underlying IPv4 interface is not in operation.

STEP 3 Click **Apply**. The tunnel is saved to the Running Configuration file.

Defining IPv6 Addresses

To assign an IPv6 address to an IPv6 Interface:

STEP 1 In Layer 2 system mode, click **Administration** > **Management Interface** > **IPv6 Addresses**.
In Layer 3 system mode, click **IP Configuration** > **IPv6 Management and Interfaces** > **IPv6 Addresses**.

STEP 2 To filter the table, select an interface name, and click **Go**. The interface appears in the IPv6 Address Table.

STEP 3 Click **Add**.

STEP 4 Enter values for the fields.

- **IPv6 Interface**—Displays the interface on which the IPv6 address is to be defined . If an * is displayed, this means that the IPv6 interface is not enabled but has been configured.
- **IPv6 Address Type**—Select the type of the IPv6 address to add.
    - *Link Local*—An IPv6 address that 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*—An IPv6 address that is a global Unicast IPV6 type that is visible and reachable from other networks.
- **IPv6 Address**—In Layer 2, the device supports a singleIPv6 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.You cannot configure an IPv6 addresses directly on an 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.

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 device default router for non-local traffic (it may be empty). The device randomly selects a router from the list. The device supports one static IPv6 default router. Dynamic default routers are routers that have sent router advertisements to the device 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 appears after an attempt is made to insert more than a single user-defined address.
- An alert message appears when attempting to insert a non-link local type address, meaning 'fe80:'.

To define a default router:

STEP 1 In Layer 2 system mode, click **Administration > Management Interface > IPv6 Default Router List**.
In Layer 3 system mode, click **IP Configuration** > **IPv6 Management and Interfaces** > **IPv6 Default Router List**.

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.

STEP 2 Click **Add** to add a static default router.

STEP 3 Enter the following fields:

- **Link Local Interface**—Displays the outgoing Link Local interface.
- **Default Router IPv6 Address**—The IP address of the default router

STEP 4 Click **Apply**. The default router is saved to the Running Configuration file.

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 device. This is the IPv6 equivalent of the IPv4 ARP Table. When the device needs to communicate with its neighbors, the device uses the IPv6 Neighbor Table to determine the MAC addresses based on their 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 In Layer 2 system mode, click **Administration > Management Interface > IPv6 Neighbors**.
In Layer 3 system mode, click **IP Configuration** > **IPv6 Management and Interfaces** > **IPv6 Neighbors**.

You can 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.
- **Router**—Specifies whether the neighbor is a router (**Yes** or **No**).

STEP 2 To add a neighbor to the table, click **Add**.

STEP 3 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 4 Click **Apply**. The Running Configuration file is updated.

STEP 5 To change the type of an IP address from **Dynamic** to **Static**, select the address, click **Edit** and use the Edit IPv6 Neighbors page.

IPv6 Prefix List

When First Hop Security is configured, it is possible to define rules for filtering based on IPv6 prefixes. These lists can be defined in the IPv6 Prefix List page.

Prefix lists are configured with **permit** or **deny** keywords to either permit or deny a prefix based on a matching condition. An implicit deny is applied to traffic that does not match any prefix-list entry.

A prefix-list entry consists of an IP address and a bit mask. The IP address can be for a classful network, a subnet, or a single host route. The bit mask is a number from 1 to 32.

Prefix lists are configured to filter traffic based on a match of an exact prefix length or a match within a range when the ge and le keywords are used.

The **Greater Than** and **Lower Than** parameters are used to specify a range of prefix lengths and provide more flexible configuration than using only the network/length argument. A prefix list is processed using an exact match when neither the **Greater Than** nor **Lower Than** parameter is specified. If only the **Greater Than** parameter is specified, the range is the value entered for **Greater Than** to a full 32-bit length. If only **Lower Than** is specified, the range is from the value entered for the network/length argument to the **Lower Than**. If both the **Greater Than** and **Lower Than** arguments are entered, the range is between the values used for **Greater Than** and **Greater Than**.

To create a prefix list:

STEP 1 (In Layer 3) Click **IP Configuration > IPv6 Management Interfaces > IPv6 Prefix List**.

-or

(In Layer 2)Click **Administration > IPv6 Management Interfaces > IPv6 Prefix List**.

STEP 2 Click **Add**.

STEP 3 Enter the following fields:

- **List Name**—Select one of the following options:
  - *Use Existing List*—Select a previously-defined list to add a prefix to it.
  - *Create New List*—Enter a name to create a new list.

- **Sequence Number**—Specifies the place of the prefix within the prefix list. Select one of the following options:
  - *Auto Numbering*—Puts the new IPV6 prefix after the last entry of the prefix list. The sequence number equals the last sequence number plus 5. If the list is empty the first prefix-list entry is assigned the number 5 and subsequent prefix list entries increment by 5.
  - *User Defined*—Puts the new IPV6 prefix into the place specified by the parameter. If an entry with the number exists, it is replaced by the new one.
- **Rule Type**—Enter the rule for the prefix list:
  - *Permit*—Permits networks that matches the condition.
  - *Deny*—Denies networks that matches the condition.
  - *Description*—Text.
- **IPv6 Prefix**—IP route prefix.
- **Prefix Length**—IP route prefix length.
- **Greater Than**—Minimum prefix length to be used for matching. Select one of the following options:
  - *No Limit*—No minimum prefix length to be used for matching.
  - *User Defined*—Minimum prefix length to be matched.
- **Lower Than**—Maximum prefix length to be used for matching. Select one of the following options:
  - *No Limit*—No maximum prefix length to be used for matching.
  - *User Defined*—Maximum prefix length to be matched.
- **Description**—Enter a description of the prefix list.

STEP 4 Click **Apply** to save the configuration to the Running Configuration file.

Viewing IPv6 Route Tables

The IPv6 Forwarding Table contains the various routes that have been configured. One of these routes is a 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 device. 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 device uses is not the router for traffic to which the IPv6 subnets that the device wants to communicate.

To view IPv6 routes:

To view IPv6 routing entries in Layer 2 system mode:

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

-or

To view IPv6 routing entries in Layer 3 system mode:
Click **IP Configuration** > **IPv6 Management and Interfaces** > **IPv6 Routes**.

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. It can be one of the following types.
    - *Link Local*—An IPv6 interface and IPv6 address that 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*—An IPv6 address that is a global Unicast IPV6 type that is visible and reachable from other networks.
    - *Point-to-Point*—A Point-to-point tunnel.
- **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.
- **Lifetime—**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 directly-connected network whose prefix is derived from a manually-configured device's IPv6 address.
  - *Dynamic*—The destination is an indirectly-attached (remote) IPv6 subnet address. The entry was obtained dynamically via the ND or ICMP protocol.
  - *Static*—The entry was manually configured by a user.

DHCPv6 Relay

DHCPv6 Relay is used for relaying DHCPv6 messages to DHCPv6 servers. It is defined in RFC 3315.

When the DHCPv6 client is not directly connected to the DHCPv6 server, a DHCPv6 relay agent (the device) to which this DHCPv6 client is directly-connected encapsulates the received messages from the directly-connected DHCPv6 client, and forwards them to the DHCPv6 server.

In the opposite direction, the relay agent decapsulates packets received from the DHCPv6 server and forwards them, towards the DHCPv6 client.

The user must configure the list DHCP servers to which packets are forwarded. Two sets of DHCPv6 servers can be configured:

- **Global Destinations**—Packets are always relayed to these DHCPv6 servers.
- **Interface List**—This is a per-interface list of DHCPv6 servers. When a DHCPv6 packet is received on an interface, the packet is relayed both to the servers on the interface list (if it exists) and to the servers on the global destination list.

Dependencies with Other Features

The DHCPv6 client and DHCPv6 relay functions are mutually exclusive on an interface.

Global Destinations

To configure a list of DHCPv6 servers to which all DHCPv6 packets are relayed:

STEP 1 Click **IP Configuration > IPv6 Management and Interfaces > DHCPv6 Relay > Global Destinations**.

STEP 2 To add a default DHCPv6 server, click **Add**.

STEP 3 Enter the fields:

- **IPv6 Address Type—**Enter the type of the destination address to which client messages are forwarded. The address type can be **Link Local**, **Global** or **Multicast** (All_DHCP_Relay_Agents_and_Servers).
- **DHCPv6 Server IP Address—**Enter the address of the DHCPv6 server to which packets are forwarded.
- **Destination IPv6 Interface—**Enter the interface on which packets are transmitted when the address type of the DHCPv6 server is **Link Local** or **Multicast**.

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

Interface Settings

To enable the DHCPv6 Relay feature on an interface and to configure a list of DHCPv6 servers to which DHCPv6 packets are relayed when they are received on this interface.

STEP 1 Click **IP Configuration > IPv6 Management and Interfaces > DHCPv6 Relay > Interface Settings**.

STEP 2 To enable DHCPv6 on an interface and optionally add a DHCPv6 server for an interface, click **Add**.

Enter the fields:

- **Source Interface—**Select the interface (port, LAG, VLAN or tunnel) for which DHCPv6 Relay is enabled.
- **Use Global Destinations Only—**Select to forward packets to the DHCPv6 global destination servers only.
- **IPv6 Address Type—**Enter the type of the destination address to which client messages are forwarded. The address type can be **Link Local**, **Global** or **Multicast** (All_DHCP_Relay_Agents_and_Servers).
- **DHCPv6 Server IP Address—**Enter the address of the DHCPv6 server to which packets are forwarded.

- **IPv6 Interface**—Enter the interface on which packets are transmitted when the address type of the DHCPv6 server is **Link Local** or **Multicast**.

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

Domain Name

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

As a DNS client, the device resolves domain names to IP addresses through the use of one or more configured DNS servers.

DNS Settings

Use the DNS Settings page to enable the DNS feature, configure the DNS servers and set the default domain used by the device.

STEP 1 Click **IP Configuration** > **Domain Name** > **DNS Settings**.

STEP 2 Enter the parameters.

- **DNS**—Select to designate the device as a DNS client, which can resolve DNS names into IP addresses through one or more configured DNS servers.
- **Polling Retries**—Enter the number of times to send a DNS query to a DNS server until the device decides that the DNS server does not exist.
- **Polling Timeout**—Enter the number of seconds that the device will wait for a response to a DNS query.
- **Polling Interval**—Enter how often (in seconds) the device sends DNS query packets after the number of retries has been exhausted.
  - *Use Default*—Select to use the default value.

    This value = 2*(Polling Retries + 1)* Polling Timeout
  - *User Defined*—Select to enter a user-defined value.
- **Default Parameters**—Enter the following default parameters:
  - **Default Domain Name**—Enter the DNS domain name used to complete unqualified host names. The device appends this to all non-fully qualified domain names (NFQDNs) turning them into FQDNs.

NOTE Do not include the initial period that separates an unqualified name from the domain name (like cisco.com).

  - **DHCP Domain Search List**—Click **Details** to view the list of DNS servers configured on the device.

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

DNS Server Table: The following fields are displayed for each DNS server configured:

- **DNS Server**—The IP address of the DNS server.
- **Preference**—Each server has a preference value, a lower value means a higher chance of being used.
- **Source**—Source of the server's IP address (static or DHCPv4 or DHCPv6)
- **Interface**—Interface of the server's IP address.

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

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 the interface through which it is received.
- **DNS Server IP Address**—Enter the DNS server IP address.
- **Preference**—Select a value that determines the order in which the domains are used (from low to high). This effectively determines the order in which unqualified names are completed during DNS queries.

STEP 5 Click **Apply**. The DNS server is saved to the Running Configuration file.

Search List

The search list can contain one static entry defined by the user the DNS Settings page and dynamic entries received from DHCPv4 and DHCPv6 servers.

To view the domain names that have been configured on the device:

STEP 1 Click **IP Configuration** > **Domain Name** > **Search List**.

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

- Domain Name—Name of domain that can be used on the device.
- **Source—**Source of the server's IP address (static or DHCPv4 or DHCPv6) for this domain.
- **Interface—**Interface of the server's IP address for this domain.
- Preference—This is the order in which the domains are used (from low to high). This effectively determines the order in which unqualified names are completed during DNS queries.

Host Mapping

Host name/IP address mappings are stored in the Host Mapping Table (DNS cache).

This cache can contain the following type of entries:

- **Static Entries—**These are mapping pairs that were manually added to the cache. There can be up to 64 static entries.
- **Dynamic Entries—**These are mapping pairs that were either added by the system as a result of being used by the user, or and an entry for each IP address configured on the device by DHCP. There can be 256 dynamic entries.

Name resolution always begins by checking static entries, continues by checking the dynamic entries, and ends by sending requests to the external DNS server.

Eight IP addresses are supported per DNS server per host name.

To add a host name and its IP address:

STEP 1 Click **IP Configuration** > **Domain Name System** > **Host Mapping**.

STEP 2 If required, select the **Clear Table** option to clear some or all of the entries in the Host Mapping Table.

- Static Only—Deletes the static hosts.
- Dynamic Only—Deletes the dynamic hosts.
- All Dynamic & Static—Deletes the static and dynamic hosts.

The Host Mapping Table displays the following fields:

- **Host Name**—User-defined host name or fully-qualified name.
- **IP Address**—The host IP address.
- **IP Version**—IP version of the host IP address.
- **Type**—Is this a **Dynamic** or **Static** entry to the cache.
- **Status**— Displays the results of attempts to access the host
    - *OK*—Attempt succeeded.
    - *Negative Cache*—Attempt failed, do not try again.
    - *No Response*—There was no response, but system can try again in future.
- **TTL**— If this is a dynamic entry, how long will it remain in the cache.
- **Remaining TTL**— If this is a dynamic entry, how much longer will it remain in the cache.

STEP 3 To add a host mapping, click **Add**.

STEP 4 Enter the parameters.

- **IP Version**—Select **Version 6** for IPv6 or **Version 4** for IPv4.
- **IPv6 Address Type**—Select the IPv6 address type (if IPv6 is used). The options are:

  - *Link Local*—The IPv6 address uniquely identifies hosts on a single network link. A link local address has a prefix of **FE80**, is not routable, and can be used for communication only on the local network. Only one link local address is supported. If a link local address exists on the interface, this entry replaces the address in the configuration.
  - *Global*—The IPv6 address is a global Unicast IPV6 type that is visible and reachable from other networks.
- **Link Local Interface**—If the IPv6 address type is Link Local, select the interface through which it is received.
- **Host Name**—Enter a user-defined host name or fully-qualified name. Host names are restricted to the ASCII letters A through Z (case-insensitive), the digits 0 through 9, the underscore and the hyphen. A period (.) is used to separate labels.
- **IP Address(es)**—Enter a single address or up to eight associated IP addresses (IPv4 or IPv6).

You can select the **Clear Table** option to clear some or all of the entries in the Host Mapping Table.

- Static Only—Deletes the static hosts.
- Dynamic Only—Deletes the dynamic hosts.
- All Dynamic & Static—Deletes the static and dynamic hosts.

18

Security

This section describes device 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 device is described in the following sections:

- **Defining Users**
- **Configuring TACACS+<300-500>**
- **Configuring RADIUS**
- **Management Access Method**
- **Management Access Method**
- **Secure Sensitive Data Management**
- **SSL Server**

Protection from attacks directed at the device CPU is described in the following sections:

- **Configuring TCP/UDP Services**
- **Defining Storm Control**
- **Access Control**

Access control of end-users to the network through the device is described in the following sections:

- **Management Access Method**
- **Management Access Method**
- **Configuring TACACS+<300-500>**

- **Configuring RADIUS**
- **Configuring Port Security**
- **802.1X**
- **Defining Time Ranges**

Protection from other network users is described in the following sections. These are attacks that pass through, but are not directed at, the device.

- **Denial of Service Prevention**
- **DHCP Snooping**
- **SSL Server**
- **Defining Storm Control**
- **Configuring Port Security**
- **IP Source Guard<300-500>**
- **ARP Inspection**
- **Access Control**
- **First Hop 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 are prompted to create another password.

Setting User Accounts

The User Accounts page enables entering additional users that are permitted to access to the device (read-only or read-write) or changing the passwords of existing users.

After adding a level 15 user (as described below), the default user is removed from the system.

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**.

This page displays the users defined in the system and their user privilege level.

STEP 2 Select **Password Recovery Service** to enable this feature. When this is enabled, an end user, with physical access to the console port of the device, can enter the boot menu and trigger the password recovery process. When the boot system process ends, you are allowed to login to the device without password authentication. Entering the device is allowed only via the console and only when the console is connected to the device with physical access.

When password recovery mechanism is disabled, accessing the boot menu is still allowed and you can trigger the password recovery process. The difference is that in this case, all configuration and user files are removed during the system boot process, and a suitable log message is generated to the terminal.

STEP 3 Click **Add** to add a new user or click **Edit** to modify a user.

STEP 4 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.
- **User Level—**Select the privilege level of the user being added/edited.
  - *Read-Only CLI Access (1)*—User cannot access the GUI, and can only access CLI commands that do not change the device configuration.
  - *Read/Limited Write CLI Access (7)*—User cannot access the GUI, and can only access some CLI commands that change the device configuration. See the *CLI Reference Guide* for more information.

- *Read/Write Management Access (15)*—User can access the GUI, and can configure the device.

STEP 5 Click **Apply**. The user is added to the Running Configuration file of the device.

Setting Password Complexity Rules

Passwords are used to authenticate users accessing the device. 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**.

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 is 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, new 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 users name or any variant reached by changing the case of the characters.

- Do not repeat or reverse the manufacturers 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.

- **Allowed Character Repetition**—Enter the number of times that a character can be repeated.
- **Minimal Number of Character Classes**—Enter the number of character classes which must be present in a password. Character classes are lower case (1), upper case (2), digits (3), and symbols or special characters (4).
- **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 written to the Running Configuration file.

NOTE Configuring the username-password equivalence, and manufacturer-password equivalence may be done through the CLI. See the *CLI Reference Guide* for further instruction.

Configuring TACACS+

An organization can establish a *Terminal Access Controller Access Control System* (TACACS+) server to provide centralized security for all of its devices. In this way, authentication and authorization can be handled on a single server for all devices in the organization.

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

- **Authentication**—Provides authentication of users logging onto the device by using usernames and user-defined passwords.

- **Authorization**—Performed at login. After the authentication session is completed, an authorization session starts using the authenticated username. The TACACS+ server then checks user privileges.
- **Accounting**—Enable accounting of login sessions using the TACACS+ server. This enables a system administrator to generate accounting reports from the TACACS+ server.

In addition to providing authentication and authorization services, the TACACS+ protocol helps to ensure TACACS message protection through encrypted TACACS body messages.

TACACS+ is supported only with IPv4.

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

Accounting Using a TACACS+ Server

The user can enable accounting of login sessions using either a RADIUS or TACACS+ server.

The user-configurable, TCP port used for TACACS+ server accounting is the same TCP port that is used for TACACS+ server authentication and authorization.

The following information is sent to the TACACS+ server by the device when a user logs in or out:

Table 2:

Argument	Description	In Start Message	In Stop Message
task_id	A unique accounting session identifier.	Yes	Yes
user	Username that is entered for login authentication.	Yes	Yes
rem-addr	P address of the user.	Yes	Yes
elapsed-time	Indicates how long the user was logged in.	No	Yes
reason	Reports why the session was terminated.	No	Yes

Defaults

The following defaults are relevant to this feature:

- No default TACACS+ server is defined by default.
- If you configure a TACACS+ server, the accounting feature is disabled by default.

Interactions With Other Features

You cannot enable accounting on both a RADIUS and TACACS+ server.

Workflow

To use a TACACS+ server, do the following:

STEP 1 Open an account for a user on the TACACS+ server.

STEP 2 Configure that server along with the other parameters in the TACACS+ and Add TACACS+ Server pages.

STEP 3 Select **TACACS+** in the Management Access Authentication page, so that when a user logs onto the device, authentication is performed on the TACACS+ server instead of in the local database.

NOTE If more than one TACACS+ server has been configured, the device uses the configured priorities of the available TACACS+ servers to select the TACACS+ server to be used by the device.

Configuring a TACACS+ Server

The TACACS+ page enables configuring TACACS+ servers.

Only users who have privilege level 15 on the TACACS+ server can administer the device. Privilege level 15 is given to a user or group of users on the TACACS+ server by the following string in the user or group definition:

```
service = exec {
priv-lvl = 15
}
```

To configure TACACS+ server parameters:

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

STEP 2 Enable TACACS+ Accounting if required. See explanation in the **Accounting Using a TACACS+ Server** section.

STEP 3 Enter the following default parameters:

- **Key String—**Enter the default **Key String** used for communicating with all TACACS+ servers in **Encrypted** or **Plaintext** mode. The device can be configured to use this key or to use a key entered for an specific server (entered in the Add TACACS+ Server page).

  If you do not enter a key string in this field, the server key entered in the Add TACACS+ Server page must match the encryption key used by the TACACS+ server.

  If you enter both a key string here and a key string for an individual TACACS+ server, the key string configured for the individual TACACS+ server takes precedence.

- **Timeout for Reply—**Enter the amount of time that passes before the connection between the device and the TACACS+ server times out. If a value is not entered in the Add TACACS+ Server page for a specific server, the value is taken from this field.

- **Source IPv4** —(In Layer 3 system mode only) Select the device IPv4 source interface to be used in messages sent for communication with the TACACS+ server.
- **Source IPv6** —(In Layer 3 system mode only) Select the device IPv6 source interface to be used in messages sent for communication with the TACACS+ server.

  NOTE If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

STEP 4 Click **Apply**. The TACACS+ default settings are added to the Running Configuration file. These are used if the equivalent parameters are not defined in the Add page.

STEP 5 To add a TACACS+ server, click **Add.**

STEP 6 Enter the parameters.

- **Server Definition—**Select one of the following ways to identify the TACACS+ server:
  - *By IP Address*—If this is selected, enter the IP address of the server in the **Server IP Address/Name** field.
  - *By Name*—If this is selected enter the name of the server in the **Server IP Address/Name** field.
- **IP Version—**Select the supported IP version of the source address: IPv6 or 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—**Select the link local interface (if IPv6 Address Type Link Local is selected) from the list.
- **Server IP Address/Name—**Enter the IP address or name of the TACACS+ server.

- **Priority—**Enter the order in which this TACACS+ server is used. Zero is the highest priority TACACS+ server and is the first server used. If it cannot establish a session with the high priority server, the device tries the next highest priority server.
- **Source IP Address—**(For SG500X devices and other devices in Layer 3 system mode). Select to use either the default device source address or one of the available device IP addresses for communication with the TACACS+ server.
- **Key String—**Enter the default key string used for authenticating and encrypting between the device and the TACACS+ server. This key must match the key configured on the TACACS+ server.

  A key string is used to encrypt communications by using MD5. You can select the default key on the device, or the key can be entered in **Encrypted** or **Plaintext** form. If you do not have an encrypted key string (from another device), enter the key string in plaintext mode and click **Apply**. The encrypted key string is generated and displayed.

  If you enter a key, this overrides the default key string if one has been defined for the device on the main page.
- **Timeout for Reply—**Enter the amount of time that passes before the connection between the device and the TACACS+ server times out. Select **Use Default** to use the default value displayed on the page.
- **IP Port—**Enter the port number through which the TACACS+ session occurs.
- **Single Connection—**Select to enable receiving all information in a single connection. If the TACACS+ server does not support this, the device reverts to multiple connections.

STEP 7 To display sensitive data in plaintext form in the configuration file, click **Display Sensitive Data As Plaintext**.

STEP 8 Click **Apply**. The TACACS+ server is added to the Running Configuration file of the device.

Configuring RADIUS

Remote Authorization Dial-In User Service (RADIUS) servers provide a centralized 802.1X or MAC-based network access control. The device is a RADIUS client that can use a RADIUS server to provide centralized security.

An organization can establish a Remote Authorization Dial-In User Service (RADIUS) server to provide centralized 802.1X or MAC-based network access control for all of its devices. In this way, authentication and authorization can be handled on a single server for all devices in the organization.

The device can act as a RADIUS client that uses the RADIUS server for the following services:

- **Authentication**—Provides authentication of regular and 802.1X users logging onto the device by using usernames and user-defined passwords.
- **Authorization**—Performed at login. After the authentication session is completed, an authorization session starts using the authenticated username. The RADIUS server then checks user privileges.
- Accounting—Enable accounting of login sessions using the RADIUS server. This enables a system administrator to generate accounting reports from the RADIUS server.

Accounting Using a RADIUS Server

The user can enable accounting of login sessions using a RADIUS server.

The user-configurable, TCP port used for RADIUS server accounting is the same TCP port that is used for RADIUS server authentication and authorization.

Defaults

The following defaults are relevant to this feature:

- No default RADIUS server is defined by default.
- If you configure a RADIUS server, the accounting feature is disabled by default.

Interactions With Other Features

You cannot enable accounting on both a RADIUS and TACACS+ server.

Radius Workflow

To user a RADIUS server, do the following:

STEP 1 Open an account for the device on the RADIUS server.

STEP 2 Configure that server along with the other parameters in the RADIUS and ADD RADIUS Server pages.

NOTE If more than one RADIUS server has been configured, the device uses the configured priorities of the available RADIUS servers to select the RADIUS server to be used by the device.

To set the RADIUS server parameters:

STEP 1 Click **Security** > **RADIUS**.

STEP 2 Enter the RADIUS Accounting option. The following options are available:

- **Port Based Access Control (802.1X, MAC Based, Web Authentication)—**Specifies that the RADIUS server is used for 802.1x port accounting.
- **Management Access—**Specifies that the RADIUS server is used for user login accounting.
- **Both Port Based Access Control and Management Access—**Specifies that the RADIUS server is used for both user login accounting and 802.1x port accounting.
- **None—**Specifies that the RADIUS server is not used for accounting.

STEP 3 Enter the default RADIUS parameters if required. Values entered in the Default Parameters are applied to all servers. If a value is not entered for a specific server (in the Add RADIUS Server page) the device uses the values in these fields.

- **Retries—**Enter the number of transmitted requests that are sent to the RADIUS server before a failure is considered to have occurred.
- **Timeout for Reply—**Enter the number of seconds that the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server.

- **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 device and the RADIUS server. This key must match the key configured on the RADIUS server. A key string is used to encrypt communications by using MD5. The key can be entered in **Encrypted** or **Plaintext** form. If you do not have an encrypted key string (from another device), enter the key string in plaintext mode and click **Apply**. The encrypted key string is generated and displayed.

This overrides the default key string if one has been defined.

- **Source IPv4** —(In Layer 3 system mode only) Select the device IPv4 source interface to be used in messages for communication with the RADIUS server.
- **Source IPv6** —(In Layer 3 system mode only) Select the device IPv6 source interface to be used in messages for communication with the RADIUS server.

  NOTE If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

STEP 4 Click **Apply**. The RADIUS default settings for the device are updated in the Running Configuration file.

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

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

- **Server Definition**—Select whether to specify the RADIUS server by IP address or name.
- **IP Version**—Select the version of the IP address of the RADIUS server.
- **IPv6 Address Type**—Displays that IPv6 address type is Global.
- **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.

- **Server IP Address/Name—**Enter the RADIUS server by IP address or name.

- **Priority—**Enter the priority of the server. The priority determines the order the device attempts to contact the servers to authenticate a user. The device starts with the highest priority RADIUS server first. Zero is the highest priority.

  Key String—Enter the key string used for authenticating and encrypting communication between the device and the RADIUS server. This key must match the key configured on the RADIUS server. It can be entered in **Encrypted** or **Plaintext** format. If **Use Default** is selected, the device attempts to authenticate to the RADIUS server by using the default Key String.

- **Timeout for Reply—**Enter the number of seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server if the maximum number of retries were made. If **Use Default** is selected, the device uses the default timeout value.

- **Authentication Port—**Enter the UDP port number of the RADIUS server port for authentication requests.

- **Accounting Port—**Enter the UDP port number of the RADIUS server port for accounting requests.

- **Retries—**Enter the number of requests that are sent to the RADIUS server before a failure is considered to have occurred. If **Use Default** is selected, the device uses the default value for the number of retries.

- **Dead Time—**Enter the number of minutes that must pass before a non-responsive RADIUS server is bypassed for service requests. If **Use Default** is selected, the device uses 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 device.

  - *802.1X*—RADIUS server is used for 802.1x authentication.

  - *All*—RADIUS server is used for authenticating user that ask to administer the device and for 802.1X authentication.

STEP 6 To display sensitive data in plaintext form in the configuration file, click **Display Sensitive Data As Plaintext**.

STEP 7 Click **Apply**. The RADIUS server definition is added to the Running Configuration file of the device.

Management Access Method

Access profiles determine how to authenticate and authorize users accessing the device through various access methods. Access Profiles can limit management access from specific sources.

Only users who pass both the active access profile and the management access authentication methods are given management access to the device.

There can only be a single access profile active on the device at one time.

Access profiles consist of one or more rules. The rules are executed in order of their priority within the access profile (top to bottom).

Rules are composed of filters that include the following elements:

- **Access Methods**—Methods for accessing and managing the device:
  - Telnet
  - Secure Telnet (SSH)
  - Hypertext Transfer Protocol (HTTP)
  - Secure HTTP (HTTPS)
  - Simple Network Management Protocol (SNMP)
  - All of the above
- **Action**—Permit or deny access to an interface or source address.
- **Interface**—Which ports, LAGs, or VLANs are permitted to access or are denied access to the web-based configuration utility.

- **Source IP Address—**IP addresses or subnets. Access to management methods might differ among user groups. For example, one user group might be able to access the device module only by using an HTTPS session, while another user group might be able to access the device module by using both HTTPS and Telnet sessions.

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 device through an access method, the device looks to see if the active access profile explicitly permits management access to the device through this method. If no match is found, access is denied.

When an attempt to access the device is in violation of the active access profile, the device generates a SYSLOG message to alert the system administrator of the attempt.

If a console-only access profile has been activated, the only way to deactivate it is through a direct connection from the management station to the physical console port on the device.

For more information see **Defining Profile Rules**.

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**.

This page displays all of the access profiles, active and inactive.

STEP 2 To change the active access profile, select a profile from the **Active Access Profile** drop down menu and click **Apply**. This makes the chosen profile the active access profile.

> **NOTE** A caution message appears if you selected Console Only. If you continue, you are immediately disconnected from the web-based configuration utility and can access the device only through the console port. This only applies to device types that offer a console port.

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

STEP 3 Click **OK** to select the active access profile or click **Cancel** to discontinue the action.

STEP 4 Click **Add** to open the Add Access Profile page. The page allows you to configure a new profile and one rule.

STEP 5 Enter the **Access Profile Name**. This name can contain up to 32 characters.

STEP 6 Enter the parameters.

- **Rule Priority—**Enter the rule priority. When the packet is matched to a rule, user groups are either granted or denied access to the device. The rule priority is essential to matching packets to rules, as packets are matched on a first-match basis. One is the highest priority.
- **Management Method**—Select the management method for which the rule is defined. The options are:
    - *All*—Assigns all management methods to the rule.
    - *Telnet*—Users requesting access to the device that meets the Telnet access profile criteria are permitted or denied access.
    - *Secure Telnet (SSH)*—Users requesting access to the device that meets the SSH access profile criteria, are permitted or denied access.
    - *HTTP*— Users requesting access to the device that meets the HTTP access profile criteria, are permitted or denied.
    - *Secure HTTP (HTTPS)*—Users requesting access to the device that meets the HTTPS access profile criteria, are permitted or denied.
    - *SNMP*—Users requesting access to the device that meets the SNMP access profile criteria are permitted or denied.
- **Action**—Select the action attached to the rule. The options are:
    - *Permit*—Permits access to the device if the user matches the settings in the profile.
    - *Deny*—Denies access to the device if the user matches the settings in the profile.
- **Applies to Interface**—Select the interface attached to the rule. The options are:

  - *All*—Applies to all ports, VLANs, and LAGs.
  - *User Defined*—Applies to selected interface.
- **Interface**—Enter the interface number if User Defined was selected.
- **Applies to Source IP Address**—Select the type of source IP address to which the access profile applies. The *Source IP Address* field is valid for a subnetwork. Select one of the following values:
  - *All*—Applies to all types of IP addresses.
  - *User Defined*—Applies to only those types of IP addresses defined in the fields.
- **IP Address**—Enter the source IP address.
- **Mask**—Select the format for the subnet mask for the source IP address, and enter a value in one of the fields:
  - *Network Mask*—Select the subnet to which the source IP address belongs and enter the subnet mask in dotted decimal format.
  - *Prefix Length*—Select the Prefix Length and enter the number of bits that comprise the source IP address prefix.

STEP 7 Click **Apply**. The access profile is written to the Running Configuration file. You can now select this access profile as the active access profile.

Defining Profile Rules

Access profiles can contain up to 128 rules to determine who is permitted to manage and access the device, and the access methods that may be used.

Each rule in an access profile contains an action and criteria (one or more parameters) to match. Each rule has a priority; rules with the lowest priority are checked first. If the incoming packet matches a rule, the action associated with the rule is performed. If no matching rule is found within the active access profile, the packet is dropped.

For example, you can limit access to the device from all IP addresses except IP addresses that are allocated to the IT management center. In this way, the device can still be managed and has gained another layer of security.

To add profile rules to an access profile:

STEP 1 Click **Security** > **Mgmt Access Method** > **Profile Rules**.

STEP 2 Select the Filter field, and an access profile. Click **Go**.

The selected access profile appears in the Profile Rule Table.

STEP 3 Click **Add** to add a rule.

STEP 4 Enter the parameters.

- **Access Profile Name—**Select an access profile.
- **Rule Priority—**Enter the rule priority. When the packet is matched to a rule, user groups are either granted or denied access to the device. The rule priority is essential to matching packets to rules, as packets are matched on a first-fit basis.
- **Management Method—**Select the management method for which the rule is defined. The options are:
    - *All*—Assigns all management methods to the rule.
    - *Telnet*—Users requesting access to the device that meets the Telnet access profile criteria are permitted or denied access.
    - *Secure Telnet (SSH)*—Users requesting access to the device that meets the Telnet access profile criteria, are permitted or denied access.
    - *HTTP*—Assigns HTTP access to the rule. Users requesting access to the device that meets the HTTP access profile criteria, are permitted or denied.
    - *Secure HTTP (HTTPS)*—Users requesting access to the device that meets the HTTPS access profile criteria, are permitted or denied.
    - *SNMP*—Users requesting access to the device that meets the SNMP access profile criteria are permitted or denied.
- **Action—**Select **Permit** to permit the users that attempt to access the device 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.

Management Access Authentication

You can assign authentication methods to the various management access methods, such as SSH, console, Telnet, HTTP, and HTTPS. The authentication can be performed locally or on a TACACS+ or RADIUS server.

For the RADIUS server to grant access to the web-based configuration utility, the RADIUS server must return cisco-avpair = shell:priv-lvl=15.

User authentication occurs in the order that the authentication methods are selected. If the first authentication method is not available, the next selected method is used. For example, if the selected authentication methods are RADIUS and Local, and all configured RADIUS servers are queried in priority order and do not reply, the user is authenticated locally.

If an authentication method fails or the user has insufficient privilege level, the user is denied access to the device. In other words, if authentication fails at an authentication method, the device stops the authentication attempt; it does not continue and does not attempt to use the next authentication method.

To define authentication methods for an access method:

STEP 1 Click **Security** > **Management Access Authentication**.

STEP 2 Select an access method from the **Application** 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.
- *TACACS+*—User authenticated on the TACACS+ server. You must have configured one or more TACACS+ servers.
- *None*—User is allowed to access the device without authentication.
- *Local*—Username and password are checked against the data stored on the local device. These username and password pairs are defined in the User Accounts page.

  NOTE The **Local** or **None** authentication method must always be selected last. All authentication methods selected after **Local** or **None** are ignored.

STEP 4 Click **Apply**. The selected authentication methods are associated with the access method.

Secure Sensitive Data Management

See **Security: Secure Sensitive Data Management**.

SSL Server

This section describes the Secure Socket Layer (SSL) feature.

SSL Overview

The Secure Socket Layer (SSL) feature is used to open an HTTPS session to the device.

An HTTPS session may be opened with the default certificate that exists on the device.

Some browsers generate warnings when using a default certificate, since this certificate is not signed by a Certification Authority (CA). It is best practice to have a certificate signed by a trusted CA.

To open an HTTPS session with a user-created certificate, perform the following actions:

1. Generate a certificate.
2. Request that the certificate be certified by a CA.
3. Import the signed certificate into the device.

Default Settings and Configuration

By default, the device contains a certificate that can be modified.

HTTPS is enabled by default.

SSL Server Authentication Settings

It may be required to generate a new certificate to replace the default certificate found on the device.

To create a new certificate:

STEP 1 Click **Security > SSL Server > SSL Server Authentication Settings.**

Information appears for certificate 1 and 2 in the SSL Server Key Table. These fields are defined in the **Edit** page except for the following fields:

- **Valid From—**Specifies the date from which the certificate is valid.

- **Valid To—**Specifies the date up to which the certificate is valid.
- **Certificate Source—**Specifies whether the certificate was generated by the system (Auto Generated) or the user (User Defined).

STEP 2 Select an active certificate.

STEP 3 Click **Generate Certificate Request**.

STEP 4 Enter the following fields:

- **Regenerate RSA Key**—Select to regenerate the RSA key.
- **Key Length**—Enter the length of the RSA key to be generated.
- **Common Name**—Specifies the fully-qualified device URL or IP address. If unspecified, defaults to the lowest IP address of the device (when the certificate is generated).
- **Organization Unit**—Specifies the organization-unit or department name.
- **Organization Name**—Specifies the organization name.
- **Location**—Specifies the location or city name.
- **State**—Specifies the state or province name.
- **Country**—Specifies the country name.
- **Duration**—Specifies the number of days a certification is valid.

STEP 5 Click **Generate Certificate Request**. This creates a key that must be entered on the Certification Authority (CA).

To import a certificate:

STEP 1 Click **Security > SSL Server > SSL Server Authentication Settings.**

STEP 2 Click **Import Certificate**.

STEP 3 Enter the following fields:

- **Certificate ID**—Select the active certificate.
- **Certificate**—Copy in the received certificate.
- **Import RSA KEY-Pair**—Select to enable copying in the new RSA key-pair.
- **Public Key**—Copy in the RSA public key.

- **Private Key (Encrypted)**—Select and copy in the RSA private key in encrypted form.
- **Private Key (Plaintext)**—Select and copy in the RSA private key in plain text form.

STEP 4 Click **Display Sensitive Data as Encrypted** to display this key as encrypted. When this button is clicked, the private keys are written to the configuration file in encrypted form (when Apply is clicked).

STEP 5 Click **Apply** to apply the changes to the Running Configuration.

The **Details** button displays the certificate and RSA key pair. This is used to copy the certificate and RSA key-pair to another device (using copy/paste). When you click **Display Sensitive Data as Encrypted**, the private keys are displayed in encrypted form.

SSH Server

See **Security: SSH Server**.

SSH Client

See **Security: SSH Client**.

Configuring TCP/UDP Services

The TCP/UDP Services page enables TCP or UDP-based services on the device, usually for security reasons.

The device offers the following TCP/UDP services:

- HTTP—Enabled by factory default
- HTTPS—Enabled by factory default
- SNMP—Disabled by factory default

- **Telnet**—Disabled by factory default
- **SSH**—Disabled by factory default

The active TCP connections are also displayed in this window.

To configure TCP/UDP services:

STEP 1 Click **Security** > **TCP/UDP Services**.

STEP 2 Enable or disable the following TCP/UDP services on the displayed services.

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

The TCP Service Table displays the following fields for each service:

- **Service Name**—Access method through which the device is offering the TCP service.
- **Type**—IP protocol the service uses.
- **Local IP Address**—Local IP address through which the device is offering the service.
- **Local Port**—Local TCP port through which the device is offering the service.
- **Remote IP Address**—IP address of the remote device that is requesting the service.
- **Remote Port**—TCP port of the remote device that is requesting the service.
- **State**—Status of the service.

The UDP Services table displays the following information:

- **Service Name**—Access method through which the device is offering the UDP service.
- **Type**—IP protocol the service uses.

- **Local IP Address**—Local IP address through which the device is offering the service.
- **Local Port**—Local UDP port through which the device is offering the service.
- **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 written to the Running Configuration file.

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 device and to define the types of frames that are counted towards this limit.

When the rate of Broadcast, Multicast, or Unknown Unicast frames is higher than the user-defined threshold, frames received beyond the threshold are discarded.

To define Storm Control:

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

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.**

STEP 3 Enter the parameters.

- **Interface**—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 four 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 device learns MAC addresses up to the configured limit of allowed addresses. After the limit is reached, the device does not learn additional addresses. In this mode, the addresses are subject to aging and re-learning.
- **Secure Permanent—**Keeps the current dynamic MAC addresses associated with the port and learns up to the maximum number of addresses allowed on the port (set by Max No. of Addresses Allowed). Relearning and aging are disabled.
- **Secure Delete on Reset—**Deletes the current dynamic MAC addresses associated with the port after reset. New MAC addresses can be learned as Delete-On-Reset ones up to the maximum addresses allowed on the port. Relearning and aging are disabled.

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 To use 802.1X on a port, it must be in multiple host or multi session modes. 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**.

STEP 2 Select an interface to be modified, and click **Edit.**

STEP 3 Enter the parameters.

- **Interface**—Select the interface name.
- **Interface Status**—Select to lock the port.
- **Learning Mode**—Select the type of port locking. To configure this field, the Interface Status must be unlocked. The Learning Mode field is enabled only if the *Interface Status* field is locked. To change the Learning Mode, the Lock Interface must be cleared. After the mode is changed, the Lock Interface can be reinstated. The options are:
    - *Classic Lock*—Locks the port immediately, regardless of the number of addresses that have already been learned.
    - *Limited Dynamic Lock*—Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both re-learning and aging of MAC addresses are enabled.

    - *Secure Permanent*—Keeps the current dynamic MAC addresses associated with the port and learns up to the maximum number of addresses allowed on the port (set by **Max No. of Addresses Allowed**). Relearning and aging are enabled.
    - *Secure Delete on Reset*—Deletes the current dynamic MAC addresses associated with the port after reset. New MAC addresses can be learned as Delete-On-Reset ones up to the maximum addresses allowed on the port. Relearning and aging are disabled.
- **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 device 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.
- **Trap Frequency**—Enter minimum time (in seconds) that elapses between traps.

STEP 4 Click **Apply**. Port security is modified, and the Running Configuration file is updated.

802.1X

See the **Security: 802.1X Authentication** chapter for information about 802.1X authentication. This includes MAC-based and web-based authentication.

Denial of Service Prevention

A Denial of Service (DoS) attack is a hacker attempt to make a device unavailable to its users.

DoS attacks saturate the device with external communication requests, so that it cannot respond to legitimate traffic. These attacks usually lead to a device CPU overload.

Secure Core Technology (SCT)

One method of resisting DoS attacks employed by the device is the use of SCT. SCT is enabled by default on the device and cannot be disabled.

The Cisco device is an advanced device that handles management traffic, protocol traffic and snooping traffic, in addition to end-user (TCP) traffic.

SCT ensures that the device receives and processes management and protocol traffic, no matter how much total traffic is received. This is done by rate-limiting TCP traffic to the CPU.

There are no interactions with other features.

SCT can be monitored in the Denial of Service > Denial of Service Prevention > Security Suite Settings page (**Details** button).

Types of DoS Attacks

The following types of packets or other strategies might be involved in a Denial of Service attack:

- **TCP SYN Packets—**These packets often have a false sender address. Each packets is handled like a connection request, causing the server to spawn a half-open connection, by sending back a TCP/SYN-ACK packet (Acknowledge), and waiting for a packet in response from the sender address (response to the ACK Packet). However, because the sender address is false, the response never comes. These half-open connections saturate the number of available connections that the device is able to make, keeping it from responding to legitimate requests.
- **TCP SYN-FIN Packets—**SYN packets are sent to create a new TCP connection. TCP FIN packets are sent to close a connection. A packet in which both SYN and FIN flags are set should never exist. Therefore these packets might signify an attack on the device and should be blocked.

- **Martian Addresses**—Martian addresses are illegal from the point of view of the IP protocol. See **Martian Addresses** for more details.
- **ICMP Attack**—Sending malformed ICMP packets or overwhelming number of ICMP packets to the victim that might lead to a system crash.
- **IP Fragmentation**—Mangled IP fragments with overlapping, over-sized payloads are sent to the device. This can crash various operating systems due to a bug in their TCP/IP fragmentation re-assembly code. Windows 3.1x, Windows 95 and Windows NT operating systems, as well as versions of Linux prior to versions 2.0.32 and 2.1.63 are vulnerable to this attack.
- **Stacheldraht Distribution**—The attacker uses a client program to connect to handlers, which are compromised systems that issue commands to zombie agents, which in turn facilitate the DoS attack. Agents are compromised via the handlers by the attacker.

  Using automated routines to exploit vulnerabilities in programs that accept remote connections running on the targeted remote hosts. Each handler can control up to a thousand agents.
- **Invasor Trojan**—A trojan enables the attacker to download a zombie agent (or the trojan may contain one). Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts. This scenario primarily concerns the device when it serves as a server on the web.
- **Back OrifaceTrojan**—This is a variation of a trojan that uses Back Oriface software to implant the trojan.

Defense Against DoS Attacks

*The Denial of Service (Do*S) Prevention feature assists the system administrator in resisting such attacks in the following ways:

- Enable TCP SYN protection. If this feature is enabled, reports are issued when a SYN packet attack is identified, and the attacked port can be temporarily shut-down. A SYN attack is identified if the number of SYN packets per second exceeds a user-configured threshold.
- Block SYN-FIN packets.
- Block packets that contain reserved Martian addresses (Martian Addresses page)

- Prevent TCP connections from a specific interface (SYN Filtering page) and rate limit the packets (SYN Rate Protection page)
- Configure the blocking of certain ICMP packets (ICMP Filtering page)
- Discard fragmented IP packets from a specific interface (IP Fragments Filtering page)
- Deny attacks from Stacheldraht Distribution, Invasor Trojan, and Back Orifice Trojan (Security Suite Settings page).

Dependencies Between Features

ACL and advanced QoS policies are not active when a port has DoS Protection enabled on it. An error message appears if you attempt to enable DoS Prevention when an ACL is defined on the interface or if you attempt to define an ACL on an interface on which DoS Prevention is enabled.

A SYN attack cannot be blocked if there is an ACL active on an interface.

Default Configuration

The DoS Prevention feature has the following defaults:

- The DoS Prevention feature is disabled by default.
- SYN-FIN protection is enabled by default (even if DoS Prevention is disabled).
- If SYN protection is enabled, the default protection mode is **Block and Report**. The default threshold is 30 SYN packets per second.
- All other DoS Prevention features are disabled by default.

Configuring DoS Prevention

The following pages are used to configure this feature.

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.

CPU Protection Mechanism: Enabled indicates that SCT is enabled.

STEP 2 Click **Details** beside **CPU Utilization** to go to the CPU Utilization page and view CPU resource utilization information.

STEP 3 Click **Edit** beside **TCP SYN Protection** to go to the SYN Protection page and enable this feature.

STEP 4 Select **DoS Prevention** to enable the feature.

- **Disable**—Disable the feature.
- **System-Level Prevention**—Enable that part of the feature that prevents attacks from Stacheldraht Distribution, Invasor Trojan, and Back Orifice Trojan.

STEP 5 If **System-Level Prevention** or **System-Level and Interface-Level Prevention** is selected, enable one or more of the following DoS Prevention options:

- **Stacheldraht Distribution**—Discards TCP packets with source TCP port equal to 16660.
- **Invasor Trojan**—Discards TCP packets with destination TCP port equal to 2140 and source TCP port equal to 1024.
- **Back Orifice Trojan**—Discards UDP packets with destination UDP port equal to 31337 and source UDP port equal to 1024.

STEP 6 Click **Apply**. The Denial of Service prevention Security Suite settings are written to the Running Configuration file.

- If Interface-Level Prevention is selected, click the appropriate **Edit** button to configure the desired prevention.

SYN Protection

The network ports might be used by hackers to attack the device in a SYN attack, which consumes TCP resources (buffers) and CPU power.

Since the CPU is protected using SCT, TCP traffic to the CPU is limited. However, if one or more ports are attacked with a high rate of SYN packets, the CPU receives only the attacker packets, thus creating Denial-of-Service.

When using the SYN protection feature, the CPU counts the SYN packets ingressing from each network port to the CPU per second.

If the number is higher than the specific, user-defined threshold, a deny SYN with MAC-to-me rule is applied on the port. This rule is unbound from the port every user-defined interval (SYN Protection Period).

To configure SYN protection:

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

STEP 2 Enter the parameters.

- **Block SYN-FIN Packets**—Select to enable the feature. All TCP packets with both SYN and FIN flags are dropped on all ports.
- **SYN Protection Mode**—Select between three modes:
    - *Disable*—The feature is disabled on a specific interface.
    - *Report*—Generates a SYSLOG message.The status of the port is changed to **Attacked** when the threshold is passed.
    - *Block and Report*—When a TCP SYN attack is identified, TCP SYN packets destined for the system are dropped and the status of the port is changed to **Blocked**.
- **SYN Protection Threshold**—Number of SYN packets per second before SYN packets will be blocked (deny SYN with MAC-to-me rule will be applied on the port).
- **SYN Protection Period**—Time in seconds before unblocking the SYN packets (the deny SYN with MAC-to-me rule is unbound from the port).

STEP 3 Click **Apply**. SYN protection is defined, and the Running Configuration file is updated.

The SYN Protection Interface Table displays the following fields for every port or LAG (as requested by the user)

- **Current Status**—Interface status. The possible values are:
    - *Normal*—No attack was identified on this interface.
    - *Blocked*—Traffic is not forwarded on this interface.
    - *Attacked*—Attack was identified on this interface.
- **Last Attack**—Date of last SYN-FIN attack identified by the system and the system action (**Reported** or **Blocked and Reported**).

Martian Addresses

The Martian Addresses page enables entering IP addresses that indicate an attack if they are seen on the network. Packets from these addresses are discarded.

The device supports a set of reserved Martian addresses that are illegal from the point of view of the IP protocol. The supported reserved Martian addresses are:

- Addresses defined to be illegal in the Martian Addresses page.
- Addresses that are illegal from the point of view of the protocol, such as loopback addresses, including addresses within the following ranges:
    - **0.0.0.0/8 (Except 0.0.0.0/32 as a Source Address)**—Addresses in this block refer to source hosts on this network.
    - **127.0.0.0/8**—Used as the Internet host loopback address.
    - **192.0.2.0/24**—Used as the TEST-NET in documentation and example codes.
    - **224.0.0.0/4 (As a Source IP Address)**—Used in IPv4 Multicast address assignments, and was formerly known as Class D Address Space.
    - **240.0.0.0/4 (Except 255.255.255.255/32 as a Destination Address)**—Reserved address range, and was formerly known as Class E Address Space.

You can also add new Martian Addresses for DoS prevention. Packets that have a Martian addresses are discarded.

To define Martian addresses:

STEP 1 Click **Security** > **Denial of Service Prevention** > **Martian Addresses**.

STEP 2 Select Reserved Martian Addresses and click **Apply** to include the reserved Martian Addresses in the System Level Prevention list.

STEP 3 To add a Martian address click **Add**.

STEP 4 Enter the parameters.

- **IP Version**—Indicates the supported IP version. Currently, support is only offered for IPv4.
- **IP Address**—Enter an IP addresses to reject. The possible values are:
    - *From Reserved List*—Select a well-known IP address from the reserved list.
    - *New IP Address*—Enter an IP address.
- **Mask**—Enter the mask of the IP address to define a range of IP addresses to reject. The values are:
    - *Network Mask*—Network mask in dotted decimal format.
    - *Prefix Length*—Enter the prefix of the IP address to define the range of IP addresses for which Denial of Service prevention is enabled.

STEP 5 Click **Apply**. The Martian addresses are written to the Running Configuration file.

SYN Filtering

The SYN Filtering page enables filtering TCP packets that contain a SYN flag, and are destined for one or more ports.

To define a SYN filter:

STEP 1 Click **Security** > **Denial of Service Prevention** > **SYN Filtering**.

STEP 2 Click **Add**.

STEP 3 Enter the parameters.

- **Interface**—Select the interface on which the filter is defined.
- **IPv4 Address**—Enter the IP address for which the filter is defined, or select *All Addresses*.
- **Network Mask**—Enter the network mask for which the filter is enabled in IP address format.
- **TCP Port**—Select the destination TCP port being filtered:
    - *Known Ports*—Select a port from the list.

  - *User Defined*—Enter a port number.
  - *All Ports*—Select to indicate that all ports are filtered.

STEP 4 Click **Apply**. The SYN filter is defined, and the Running Configuration file is updated.

SYN Rate Protection

The SYN Rate Protection page enables limiting the number of SYN packets received on the ingress port. This can mitigate the effect of a SYN flood against servers, by rate limiting the number of new connections opened to handle packets.

This feature is only available when the device is in Layer 2 system mode.

To define SYN rate protection:

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

This page appears the SYN rate protection currently defined per interface.

STEP 2 Click **Add**.

STEP 3 Enter the parameters.

- **Interface**—Select the interface on which the rate protection is being defined.
- **IP Address**—Enter the IP address for which the SYN rate protection is defined or select *All Addresses*. If you enter the IP address, enter either the mask or prefix length.
- **Network Mask**—Select the format for the subnet mask for the source IP address, and enter a value in one of the field:
  - *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.
- **SYN Rate Limit**—Enter the number of SYN packets that be received.

STEP 4 Click **Apply**. The SYN rate protection is defined, and the Running Configuration is updated.

ICMP Filtering

The ICMP Filtering page enables the blocking of ICMP packets from certain sources. This can reduce the load on the network in case of an ICMP attack.

To define ICMP filtering:

STEP 1 Click **Security** > **Denial of Service Prevention** > **ICMP Filtering**.

STEP 2 Click **Add**.

STEP 3 Enter the parameters.

- **Interface**—Select the interface on which the ICMP filtering is being defined.
- **IP Address**—Enter the IPv4 address for which the ICMP packet filtering is activated or select *All Addresses* to block ICMP packets from all source addresses. If you enter the IP address, enter either the mask or prefix length.
- **Network Mask**—Select the format for the subnet mask for the source IP address, and enter a value in one of the field:
  - *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 4 Click **Apply**. The ICMP filtering is defined, and the Running Configuration is updated.

IP Fragmented Filtering

The IP Fragmented page enables blocking fragmented IP packets.

To configure fragmented IP blocking:

STEP 1 Click Security > Denial of Service Prevention > IP Fragments Filtering.

STEP 2 Click Add.

STEP 3 Enter the parameters.

- **Interface—**Select the interface on which the IP fragmentation is being defined.
- **IP Address—**Enter an IP network from which the fragmented IP packets is filtered or select *All Addresses* to block IP fragmented packets from all addresses. If you enter the IP address, enter either the mask or prefix length.
- **Network Mask—**Select the format for the subnet mask for the source IP address, and enter a value in one of the field:
  - *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 4 Click **Apply**. The IP fragmentation is defined, and the Running Configuration file is updated.

DHCP Snooping

See **DHCPv4 Snooping/Relay<300-500>**.

IP Source Guard

IP Source Guard is a security feature that can be used to prevent traffic attacks caused when a host tries to use the IP address of its neighbor.

When IP Source Guard is enabled, the device only transmits client IP traffic to IP addresses contained in the DHCP Snooping Binding database. This includes both addresses added by DHCP Snooping and manually-added entries.

If the packet matches an entry in the database, the device forwards it. If not, it is dropped.

Interactions with Other Features

The following points are relevant to IP Source Guard:

- DHCP Snooping must be globally enabled in order to enable IP Source Guard on an interface.
- IP source guard can be active on an interface only if:
  - DHCP Snooping is enabled on at least one of the port's VLANs
  - The interface is DHCP untrusted. All packets on trusted ports are forwarded.
- If a port is DHCP trusted, filtering of static IP addresses can be configured, even though IP Source Guard is not active in that condition by enabling IP Source Guard on the port.
- When the ports status changes from DHCP untrusted to DHCP trusted, the static IP address filtering entries remain in the Binding database, but they become inactive.
- Port security cannot be enabled if source IP and MAC address filtering is configured on a port.
- IP Source Guard uses TCAM resources and requires a single TCAM rule per IP Source Guard address entry. If the number of IP Source Guard entries exceeds the number of available TCAM rules, the extra addresses are inactive.

Filtering

If IP Source Guard is enabled on a port then:

- DHCP packets allowed by DHCP Snooping are permitted.
- If source IP address filtering is enabled:
  - IPv4 traffic: Only traffic with a source IP address that is associated with the port is permitted.
  - Non IPv4 traffic: Permitted (Including ARP packets).

Configuring IP Source Guard Work Flow

To configure IP Source Guard:

STEP 1 Enable DHCP Snooping in the IP Configuration > DHCP > Properties page or in the Security > DHCP Snooping > Properties page.

STEP 2 Define the VLANs on which DHCP Snooping is enabled in the IP Configuration > DHCP > Interface Settings page.

STEP 3 Configure interfaces as trusted or untrusted in the IP Configuration > DHCP > DHCP Snooping Interface page.

STEP 4 Enable IP Source Guard in the Security > IP Source Guard > Properties page.

STEP 5 Enable IP Source Guard on the untrusted interfaces as required in the Security > IP Source Guard > Interface Settings page.

STEP 6 View entries to the Binding database in the Security > IP Source Guard > Binding Database page.

Enabling IP Source Guard

To enable IP Source Guard globally:

STEP 1 Click **Security** > **IP Source Guard** > **Properties**.

STEP 2 Select **Enable** to enable IP Source Guard globally.

Configuring IP Source Guard on Interfaces

If IP Source Guard is enabled on an untrusted port/LAG, DHCP packets, allowed by DHCP Snooping, are transmitted. If source IP address filtering is enabled, packet transmission is permitted as follows:

- **IPv4 traffic —** Only IPv4 traffic with a source IP address that is associated with the specific port is permitted.
- **Non IPv4 traffic —** All non-IPv4 traffic is permitted.

See **Interactions with Other Features** for more information about enabling IP Source Guard on interfaces.

To configure IP Source Guard on interfaces:

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

STEP 2 Select port/LAG from the **Filter** field and click **Go**. The ports/LAGs on this unit are displayed along with the following:

- IP Source Guard —Indicates whether IP Source Guard is enabled on the port.
- DHCP Snooping Trusted Interface—Indicates whether this is a DHCP trusted interface.

STEP 3 Select the port/LAG and click **Edit**. Select **Enable** in the **IP Source Guard** field to enable IP Source Guard on the interface.

STEP 4 Click **Apply** to copy the setting to the Running Configuration file.

Binding Database

IP Source Guard uses the DHCP Snooping Binding database to check packets from untrusted ports. If the device attempts to write too many entries to the DHCP Snooping Binding database, the excessive entries are maintained in an inactive status. Entries are deleted when their lease time expires and so inactive entries may be made active.

See **DHCPv4 Snooping/Relay<300-500>**.

NOTE The Binding Database page **only** displays the entries in the DHCP Snooping Binding database defined on IP-Source-Guard-enabled ports.

To view the DHCP Snooping Binding database and see TCAM usage, set **Insert Inactive**:

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

STEP 2 The DHCP Snooping Binding database uses TCAM resources for managing the database. Complete the **Insert Inactive** field to select how frequently the device should attempt to activate inactive entries. It has the following options:

- **Retry Frequency—**The frequency with which the TCAM resources are checked.
- **Never**-Never try to reactivate inactive addresses.

STEP 3 Click Apply to save the above changes to the Running Configuration and/or Retry Now to check TCAM resources.

The entries in the Binding database are displayed:

- **VLAN ID**—VLAN on which packet is expected.
- **MAC Address**—MAC address to be matched.
- **IP Address**—IP address to be matched.
- **Interface**—Interface on which packet is expected.
- **Status**—Displays whether interface is active.
- **Type**—Displays whether entry is dynamic or static.
- **Reason**—If the interface is not active, displays the reason. The following reasons are possible:
  - *No Problem*—Interface is active.
  - *No Snoop VLAN*—DHCP Snooping is not enabled on the VLAN.
  - *Trusted Port*—Port has become trusted.
  - *Resource Problem*—TCAM resources are exhausted.

To see a subset of these entries, enter the relevant search criteria and click **Go**.

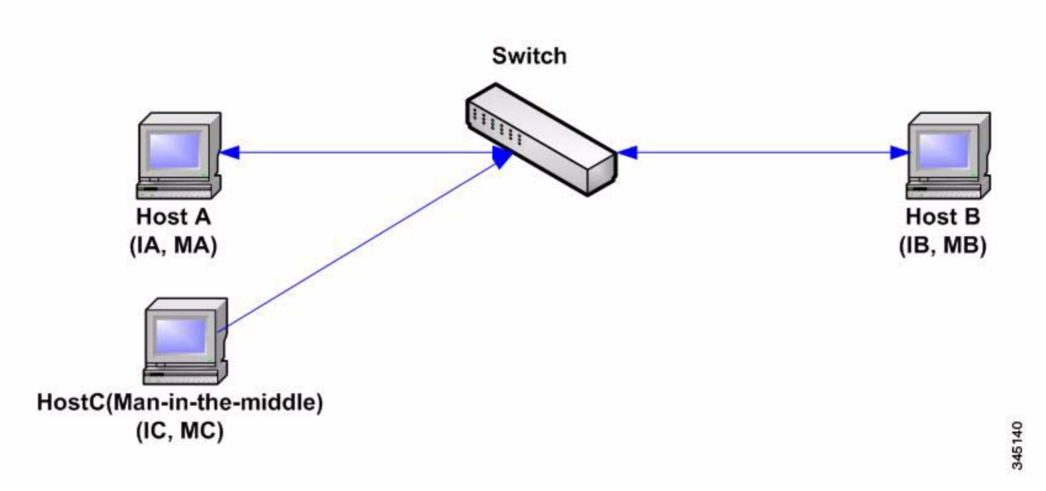
ARP Inspection

ARP enables IP communication within a Layer 2 Broadcast domain by mapping IP addresses to a MAC addresses.

A malicious user can attack hosts, switches, and routers connected to a Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. This can happen because ARP allows a gratuitous reply from a host even if an ARP request was not received. After the attack, all traffic from the device under attack flows through the attacker's computer and then to the router, switch, or host.

The following shows an example of ARP cache poisoning.

ARP Cache Poisoning



Hosts A, B, and C are connected to the switch on interfaces A, B and C, all of which are on the same subnet. Their IP, MAC addresses are shown in parentheses; for example, Host A uses IP address IA and MAC address MA. When Host A needs to communicate with Host B at the IP layer, it broadcasts an ARP request for the MAC address associated with IP address IB. Host B responds with an ARP reply. The switch and Host A update their ARP cache with the MAC and IP of Host B.

Host C can poison the ARP caches of the switch, Host A, and Host B by broadcasting forged ARP responses with bindings for a host with an IP address of IA (or IB) and a MAC address of MC. Hosts with poisoned ARP caches use the MAC address MC as the destination MAC address for traffic intended for IA or IB, which enables Host C intercepts that traffic. Because Host C knows the true MAC addresses associated with IA and IB, it can forward the intercepted traffic to those hosts by using the correct MAC address as the destination. Host C has inserted itself into the traffic stream from Host A to Host B, the classic man-in-the-middle attack.

How ARP Prevents Cache Poisoning

The ARP inspection feature relates to interfaces as either trusted or untrusted (see Security > ARP Inspection > Interface Setting page).

Interfaces are classified by the user as follows:

- **Trusted —** Packets are not inspected.
- **Untrusted —**Packets are inspected as described above.

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

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

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

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

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

Packets with invalid ARP Inspection bindings are logged and dropped.

Up to 1024 entries can be defined in the ARP Access Control table.

Interaction Between ARP Inspection and DHCP Snooping

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

ARP Defaults

The following table describes the ARP defaults:

Option	Default State
Dynamic ARP Inspection	Not enabled.
ARP Packet Validation	Not enabled
ARP Inspection Enabled on VLAN	Not enabled
Log Buffer Interval	SYSLOG message generation for dropped packets is enabled at 5 seconds interval

ARP Inspection Work Flow

To configure ARP Inspection:

STEP 1 Enable ARP Inspection and configure various options in the Security > ARP Inspection > Properties page.

STEP 2 Configure interfaces as ARP trusted or untrusted in the Security > ARP Inspection > Interface Setting page.

STEP 3 Add rules in the Security > ARP Inspection > ARP Access Control and ARP Access Control Rules pages.

STEP 4 Define the VLANs on which ARP Inspection is enabled and the Access Control Rules for each VLAN in the Security > ARP Inspection > VLAN Settings page.

Defining ARP Inspection Properties

To configure ARP Inspection:

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

Enter the following fields:

- **ARP Inspection Status**—Select to enable ARP Inspection.
- ARP Packet Validation—Select to enable the following validation checks:
  - **Source MAC —** Compares the packets source MAC address in the Ethernet header against the senders MAC address in the ARP request. This check is performed on both ARP requests and responses.
  - **Destination MAC —** Compares the packets destination MAC address in the Ethernet header against the destination interfaces MAC address. This check is performed for ARP responses.
  - **IP Addresses —** Compares the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP Multicast addresses.
- Log Buffer Interval—Select one of the following options:
  - **Retry Frequency**—Enable sending SYSLOG messages for dropped packets. Entered the frequency with which the messages are sent.
  - **Never**—Disabled SYSLOG dropped packet messages.

STEP 2 Click **Apply**. The settings are defined, and the Running Configuration file is updated.

Defining Dynamic ARP Inspection Interfaces Settings

Packets from untrusted ports/LAGs are checked against the ARP Access Rules table and the DHCP Snooping Binding database if DHCP Snooping is enabled (see the DHCP Snooping Binding Database page).

By default, ports/LAGs are ARP Inspection untrusted.

To change the ARP trusted status of a port/LAG:

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

The ports/LAGs and their ARP trusted/untrusted status are displayed.

STEP 2 To set a port/LAG as untrusted, select the port/LAG and click **Edit**.

STEP 3 Select **Trusted** or **Untrusted** and click **Apply** to save the settings to the Running Configuration file.

Defining ARP Inspection Access Control

To add entries to the ARP Inspection table:

STEP 1 Click **Security** > **ARP Inspection** > **ARP Access Control**.

STEP 2 To add an entry, click **Add**.

STEP 3 Enter the fields:

- **ARP Access Control Name**—Enter a user-created name.
- **MAC Address**—MAC address of packet.
- **IP Address**—IP address of packet.

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

Defining ARP Inspection Access Control Rules

To add more rules to a previously-created ARP Access Control group:

STEP 1 Click **Security** > **ARP Inspection** > **ARP Access Control Rules**.

The currently-defined access rules are displayed.

STEP 2 To add more rules to a group, click **Add**.

STEP 3 Select a Access Control Group and enter the fields:

- **MAC Address**—MAC address of packet.
- **IP Address**—IP address of packet.

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

Defining ARP Inspection VLAN Settings

To enable ARP Inspection on VLANs and associate Access Control Groups with a VLAN:

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

STEP 2 To enable ARP Inspection on a VLAN, move the VLAN from the **Available VLANs** list to the **Enabled VLANs** list.

STEP 3 To associate an ARP Access Control group with a VLAN, click **Add**. Select the VLAN number and select a previously-defined **ARP Access Control** group.

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

First Hop Security

Security: IPV6 First Hop Security

19

Security: 802.1X Authentication

This section describes 802.1X authentication.

It covers the following topics:

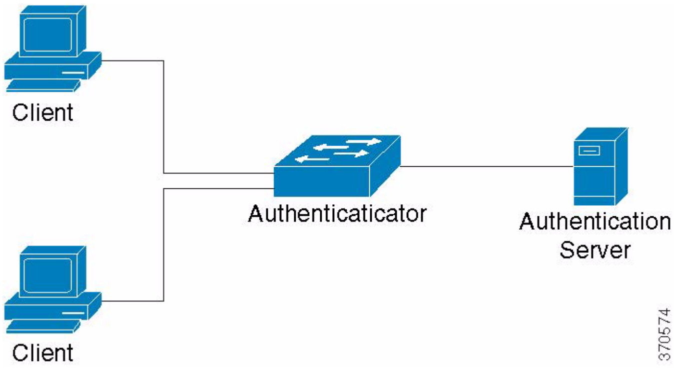
- **Overview of 802.1X**
- **Authenticator Overview**
- **Common Tasks**
- **802.1X Configuration Through the GUI**
- **Defining Time Ranges<300-500>**
- **Authentication Method and Port Mode Support<300-500>**

Overview of 802.1X

802.1x authentication restricts unauthorized clients from connecting to a LAN through publicity-accessible ports. 802.1x authentication is a client-server model. In this model, network devices have the following specific roles.

- Client or supplicant
- Authenticator
- Authentication server

This is described in the figure below:



A network device can be either a client/supplicant, authenticator or both per port.

Client or Supplicant

A client or supplicant is a network device that requests access to the LAN. The client is connected to an authenticator.

If the client uses the 802.1x protocol for authentication, it runs the supplicant part of the 802.1x protocol and the client part of the EAP protocol.

No special software is required on the client to use MAC-based or web-based authentication.

Authenticator

An authenticator is a network device that provides network services and to which supplicant ports are connected.

The following authentication modes on ports are supported (these modes are set in Security > 802.1X/MAC/Web Authentication > Host and Authentication):

- **Single-host**—Supports port-based authentication with a single client per port.
- **Multi-host**—Supports port-based authentication with a multiple clients per port.
- **Multi-sessions**—Supports client-based authentication with a multiple clients per port.

See **Port Host Modes** for more information.

The following authentication methods are supported:

- **802.1x-based**—Supported in all authentication modes.
- **MAC-based**—Supported in all authentication modes.
- **WEB-based**—Supported only in multi-sessions modes.

In 802.1x-based authentication, the authenticator extracts the EAP messages from the 802.1x messages (EAPOL frames) and passes them to the authentication server, using the RADIUS protocol.

With MAC-based or web-based authentication, the authenticator itself executes the EAP client part of the software.

Authentication Server

An authentication server performs the actual authentication of the client. The authentication server for the device is a RADIUS authentication server with EAP extensions.

Authenticator Overview

Port Administrative Authentication States

The port administrative state determines whether the client is granted access to the network.

The port administrative state can be configured in the Security > 802.1X/MAC/Web Authentication > Port Authentication page.

The following values are available:

- **force-authorized**

  Port authentication is disabled and the port transmits all traffic in accordance with its static configuration without requiring any authentication. The switch sends the 802.1x EAP-packet with the EAP success message inside when it receives the 802.1x EAPOL-start message.

  This is the default state.

- force-unauthorized

  Port authentication is disabled and the port transmits all traffic via the guest VLAN and unauthenticated VLANs. For more information see **Defining Host and Session Authentication**. The switch sends 802.1x EAP packets with EAP failure messages inside when it receives 802.1x EAPOL-Start messages.

- auto

  Enables 802.1 x authentications in accordance with the configured port host mode and authentication methods configured on the port.

Port Host Modes

Ports can be placed in the following port host modes (configured in the Security > 802.1X/MAC/Web Authentication > Host and Authentication page):

- Single-Host Mode

  A port is authorized if there is an authorized client. Only one host can be authorized on a port.

  When a port is unauthorized and the guest VLAN is enabled, untagged traffic is remapped to the guest VLAN. Tagged traffic is dropped unless it belongs to the guest VLAN or to an unauthenticated VLAN. If a guest VLAN is not enabled on the port, only tagged traffic belonging to the unauthenticated VLANs is bridged.

  When a port is authorized, untagged and tagged traffic from the authorized host is bridged based on the static VLAN membership port configuration. Traffic from other hosts is dropped.

  A user can specify that untagged traffic from the authorized host will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. Tagged traffic is dropped unless it belongs to the RADIUS-assigned VLAN or the unauthenticated VLANs. Radius VLAN assignment on a port is set in the Security > 802.1X/MAC/Web Authentication > Port Authentication page.

- Multi-Host Mode

  A port is authorized if there is if there is at least one authorized client.

When a port is unauthorized and a guest VLAN is enabled, untagged traffic is remapped to the guest VLAN. Tagged traffic is dropped unless it belongs to the guest VLAN or to an unauthenticated VLAN. If guest VLAN is not enabled on a port, only tagged traffic belonging to unauthenticated VLANs is bridged.

When a port is authorized, untagged and tagged traffic from all hosts connected to the port is bridged, based on the static VLAN membership port configuration.

You can specify that untagged traffic from the authorized port will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. Tagged traffic is dropped unless it belongs to the RADIUS-assigned VLAN or to the unauthenticated VLANs. Radius VLAN assignment on a port is set in the Port Authentication page.

- Multi-Sessions Mode

  Unlike the single-host and multi-host modes, a port in the multi-session mode does not have an authentication status. This status is assigned to each client connected to the port. This mode requires a TCAM lookup. Since Layer 3 mode switches (see **Multi-Sessions Mode Support**) do not have a TCAM lookup allocated for multi-sessions mode, they support a limited form of multi-sessions mode, which does not support guest VLAN and RADIUS VLAN attributes. The maximum number of authorized hosts allowed on the port is configured in the Port Authentication page.

  Tagged traffic belonging to an unauthenticated VLAN is always bridged regardless of whether the host is authorized or not.

  Tagged and untagged traffic from unauthorized hosts not belonging to an unauthenticated VLAN is remapped to the guest VLAN if it is defined and enabled on the VLAN, or is dropped if the guest VLAN is not enabled on the port.

  If an authorized host is assigned a VLAN by a RADIUS server, all its tagged and untagged traffic not belonging to the unauthenticated VLANs is bridged via the VLAN; if the VLAN is not assigned, all its traffic is bridged based on the static VLAN membership port configuration.

The Sx300 in Layer 3 router mode supports the multi-sessions mode without guest VLAN and RADIUS-VLAN assignment:

Multiple Authentication Methods

If more than one authentication method is enabled on the switch, the following hierarchy of authentication methods is applied:

- 802.1x Authentication: Highest
- WEB-Based Authentication
- MAC-Based Authentication: Lowest

Multiple methods can run at the same time. When one method finishes successfully, the client becomes authorized, the methods with lower priority are stopped and the methods with higher priority continue.

When one of authentication methods running simultaneously fails, the other methods continue.

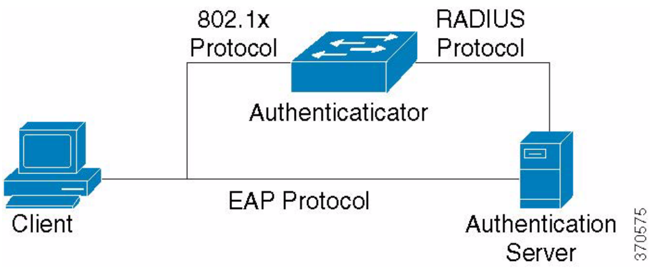
When an authentication method finishes successfully for a client authenticated by an authentication method with a lower priority, the attributes of the new authentication method are applied. When the new method fails, the client is left authorized with the old method.

802.1x-Based Authentication

The 802.1x-based authenticator relays transparent EAP messages between 802.1x supplicants and authentication servers. The EAP messages between supplicants and the authenticator are encapsulated into the 802.1x messages, and the EAP messages between the authenticator and authentication servers are encapsulated into the RADIUS messages.

This is described in the following:

Figure 1 802.1x-Based Authentication

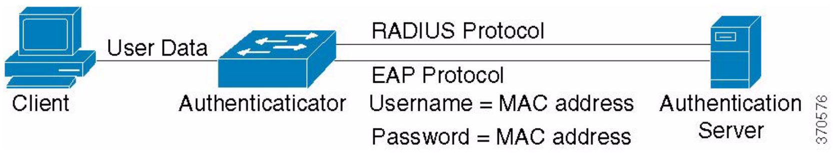


MAC-Based Authentication

MAC-based authentication is an alternative to 802.1X authentication that allows network access to devices (such as printers and IP phones) that do not have the 802.1X supplicant capability. MAC-based authentication uses the MAC address of the connecting device to grant or deny network access.

In this case, the switch supports EAP MD5 functionality with the username and password equal to the client MAC address, as shown below.

Figure 2 MAC-Based Authentication



The method does not have any specific configuration.

WEB-Based Authentication

WEB-based authentication is used to authenticate end users who request access to a network through a switch. It enables clients directly connected to the switch to be authenticated using a captive-portal mechanism before the client is given access to the network. Web-based authentication is client-based authentication and is supported in the multi-sessions mode in both Layer 2 and Layer 3.

This method of authentication is enabled per port, and when a port is enabled, each host must authenticate itself in order to access the network. So on an enabled port, you can have authenticated and unauthenticated hosts.

When web-based authentication is enabled on a port, the switch drops all traffic coming onto the port from unauthorized clients, except for ARP, DHCP, DNS and NETBIOS packets. These packets are allowed to be forwarded by the switch so that even unauthorized clients can get an IP address and be able to resolve the host or domain names.

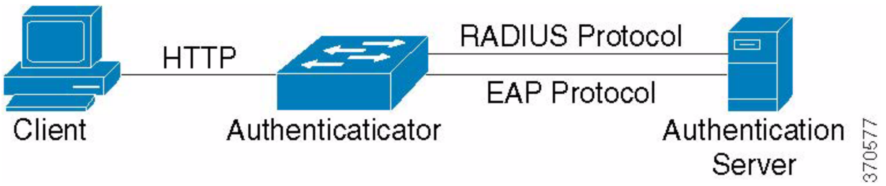
All HTTP/HTTPS over IPv4 packets from unauthorized clients are trapped to the CPU on the switch. When an end user requests access to the network, if Web-based authentication is enabled on the port, a login page is displayed, before the requested page is displayed. The user must enter his username/password, which is authenticated by a RADIUS server using the EAP protocol. If authentication is successful, the user is informed.

The user now has an authenticated session. The session remains open while it is being used. If it is not used for a specific time interval, the session is closed . This time interval is configured by the system administrator and is called Quiet Time. When the session is timed-out, the username/password is discarded, and the guest must re-enter them to open a new session.

See **Table 1 Port Modes and Authentication Methods**.

After authentication is completed, the switch forwards all traffic arriving from the client on the port, as shown in the figure below.

Figure 3 WEB-Based Authentication



Web-based authentication cannot be configured on a port that has the guest VLAN or RADIUS-Assigned VLAN feature enabled.

Web-based authentication supports the following pages:

- Login page
- Login Success page

There is a predefined, embedded set of these pages.

These pages can be modified in the Security > 802.1X/MAC/Web Authentication > Web Authentication Customization page.

You can preview each of the customized pages. The configuration is saved into the Running Configuration file.

The following table describes which SKUs support web-based authentication and in which system modes:

SKU	System Mode	WBA Supported
Sx300	**Layer 2**	Yes
	Layer 3	No
Sx500, Sx500ESW2-550X	**Layer 2**	Yes
	Layer 3	No

SKU	System Mode	WBA Supported
SG500X	**Native**	Yes
	Basic Hybrid - Layer 2	Yes
	Basic Hybrid - Layer 3	No
SG500XG	**Same as Sx500**	Yes

NOTE

- When web-based authentication is not supported, guest VLAN and DVA cannot be configured in multi-session mode.
- When web-based authentication is supported, guest VLAN and DVA can be configured in multi-session mode

Unauthenticated VLANs and the Guest VLAN

Unauthenticated VLANs and the guest VLAN provide access to services that do not require the subscribing devices or ports to be 802.1X or MAC-Based authenticated and authorized.

The guest VLAN is the VLAN that is assigned to an unauthorized client. You can configure the guest VLAN and one or more VLANs to be unauthenticated in the Security > 802.1X/MAC/Web Authentication > Properties page.

An unauthenticated VLAN is a VLAN that allows access by both authorized and unauthorized devices or ports.

An unauthenticated VLAN has the following characteristics:

- It must be a static VLAN, and cannot be the guest VLAN or the default VLAN.
- The member ports must be manually configured as tagged members.
- The member ports must be trunk and/or general ports. An access port cannot be member of an unauthenticated VLAN.

The guest VLAN, if configured, is a static VLAN with the following characteristics:

- It must be manually defined from an existing static VLAN.
- The guest VLAN cannot be used as the Voice VLAN or an unauthenticated VLAN.

See **"Table 3 Guest VLAN Support and RADIUS-VLAN Assignment Support"** to see a summary of the modes in which guest VLAN is supported.

Host Modes with Guest VLAN

The host modes work with guest VLAN in the following way:

- Single-Host and Multi-Host Mode

  Untagged traffic and tagged traffic belonging to the guest VLAN arriving on an unauthorized port are bridged via the guest VLAN. All other traffic is discarded. The traffic belonging to an unauthenticated VLAN is bridged via the VLAN.

- Multi-Sessions Mode in Layer 2

  Untagged traffic and tagged traffic, which does not belong to the unauthenticated VLANs and that arrives from unauthorized clients, are assigned to the guest VLAN using the TCAM rule and are bridged via the guest VLAN. The tagged traffic belonging to an unauthenticated VLAN is bridged via the VLAN.

  This mode cannot be configured on the same interface with policy-based VLANs.

- Multi-Sessions Mode in Layer 3

  The mode does not support the guest VLAN.

RADIUS VLAN Assignment or Dynamic VLAN Assignment

An authorized client can be assigned a VLAN by the RADIUS server, if this option is enabled in the Port Authentication page. This is called either Dynamic VLAN Assignment (DVA) or RADIUS-Assigned VLAN. In this guide, the term RADIUS-Assigned VLAN is used.

When a port is in multi-session mode and RADIUS-Assigned VLAN is enabled, the device automatically adds the port as an untagged member of the VLAN that is assigned by the RADIUS server during the authentication process. The device classifies untagged packets to the assigned VLAN if the packets originated from the devices or ports that are authenticated and authorized.

See **Table 3 Guest VLAN Support and RADIUS-VLAN Assignment Support** and **The following table describes how authenticated and non-authenticated traffic is handled in various situations.** for further information about how the different modes behave when RADIUS-Assigned VLAN is enabled on the device.

NOTE . In multi-session mode, RADIUS VLAN assignment is only supported when the device is in Layer 2 system mode.

For a device to be authenticated and authorized at a port which is DVA-enabled:

- The RADIUS server must authenticate the device and dynamically assign a VLAN to the device. You can set the RADIUS VLAN Assignment field to static in the Port Authentication page. This enables the host to be bridged according to static configuration.
- A RADIUS server must support DVA with RADIUS attributes tunnel-type (64) = VLAN (13), tunnel-media-type (65) = 802 (6), and tunnel-private-group-id = a VLAN ID.

When the RADIUS-Assigned VLAN feature is enabled, the host modes behave as follows:

- Single-Host and Multi-Host Mode

  Untagged traffic and tagged traffic belonging to the RADIUS-assigned VLAN are bridged via this VLAN. All other traffic not belonging to unauthenticated VLANs is discarded.

- Full Multi-Sessions Mode

  Untagged traffic and tagged traffic not belonging to the unauthenticated VLANs arriving from the client are assigned to the RADIUS-assigned VLAN using TCAM rules and are bridged via the VLAN.

- Multi-Sessions Mode in Layer 3 System Mode

  This mode does not support RADIUS-assigned VLAN,

The following table describes guest VLAN and RADIUS-VLAN assignment support depending on authentication method and port mode.

Authentication Method	Single-host	Multi-host	Multi-sessions	
			Device in L3	Device in L2
802.1x	†	†	N/S	†
MAC	†	†	N/S	†
WEB	N/S	N/S	N/S	N/S

Legend:

†—The port mode supports the guest VLAN and RADIUS-VLAN assignment

N/S—The port mode does not support the authentication method.

Violation Mode

In single-host mode you can configure the action to be taken when an unauthorized host on authorized port attempts to access the interface. This is done in the Host and Session Authentication page.

The following options are available:

- **restrict**—Generates a trap when a station, whose MAC address is not the supplicant MAC address, attempts to access the interface. The minimum time between the traps is 1 second. These frames are forwarded, but their source addresses are not learned.
- **protect**—Discard frames with source addresses that are not the supplicant address.
- **shutdown**—Discard frames with source addresses that are not the supplicant address and shutdown the port.

You can also configure the device to send SNMP traps, with a configurable minimum time between consecutive traps. If seconds = 0, traps are disabled. If minimum time is not specified, it defaults to 1 second for the restrict mode and 0 for the other modes.

Quiet Period

The Quiet period is a period when the port (single-host or multi-host modes) or the client (multi-sessions mode) cannot attempt authentication, following a failed authentication exchange. In single-host or multi-host mode, the period is defined per port, and in the multi-sessions mode the period is defined per client. During the quiet period, the switch does not accept or initiate authentication requests.

The period is only applied to 802.1x-based and Web-based authentications.

You can also specify the maximum number of login attempts before the quiet period is started. A value of 0 specifies the unlimited number of login attempts.

The duration of the quiet period and the maximum number of login attempts can be set in the Port Authentication page.

Common Tasks

Workflow 1: To enable 802.1x authentication on a port:

STEP 1 Click Security > 802.1X/MAC/Web Authentication > Properties.

STEP 2 Enable Port-based Authentication.

STEP 3 Select the Authentication Method .

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

STEP 5 Click Security > 802.1X/MAC/Web Authentication> Host and Session.

STEP 6 Select the required port and click Edit.

STEP 7 Set the Host Authentication mode.

STEP 8 Click **Apply**, and the Running Configuration file is updated.

STEP 9 Click Security > 802.1X/MAC/Web Authentication > Port Authentication.

STEP 10 Select a port, and click **Edit**.

STEP 11 Set the Administrative Port Control field to Auto.

STEP 12 Define the authentication methods.

STEP 13 Click **Apply**, and the Running Configuration file is updated.

Workflow 2: To configure traps

STEP 1 Click **Security** > **802.1X/MAC/Web Authentication** > **Properties**.

STEP 2 Select the required traps.

STEP 3 Click **Apply**, and the Running Configuration file is updated.

Workflow 3: To configure 802.1x-based or Web-based authentication

STEP 1 Click Security > 802.1X/MAC/Web Authentication > Port Authentication .

STEP 2 Select the required port and click Edit.

STEP 3 Enter the fields required for the port.

The fields in this page are described in **Defining 802.1X Port Authentication**.

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

Use the **Copy Settings** button to copy settings from one port to another.

Workflow 4: To configure the quiet period

STEP 1 Click **Security** > **802.1X/MAC/Web Authentication** > **Port Authentication** .

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

STEP 3 Enter the quiet period in the Quiet Period field.

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

Workflow 5: To configure the guest VLAN:

STEP 1 Click **Security** > **802.1X/MAC/Web Authentication** > **Properties**.

STEP 2 Select **Enable** in the Guest VLAN field.

STEP 3 Select the guest VLAN in the Guest VLAN ID field.

STEP 4 Configure the Guest VLAN Timeout to be either Immediate or enter a value in the User defined field.

STEP 5 Click **Apply**, and the Running Configuration file is updated.

Workflow 6: To configure unauthenticated VLANs

STEP 1 Click **Security** > **802.1X/MAC/Web Authentication** > **Properties**.

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

STEP 3 Select a VLAN.

STEP 4 Optionally, uncheck **Authentication** to make the VLAN an unauthenticated VLAN.

STEP 5 Click **Apply**, and the Running Configuration file is updated.

802.1X Configuration Through the GUI

Defining 802.1X Properties

The 802.1X Properties page is used to globally enable 802.1X and define how ports are 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/MAC/Web Authentication > **Properties**.

STEP 2 Enter the parameters.

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

  If this is disabled 802.1X, MAC-based and web-based authentication is disabled.

- **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. If the server is available but the user credentials are incorrect, access is denied and the session terminated.
  - *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.
- **Guest VLAN**—Select to enable the use of a guest VLAN for unauthorized ports. If a guest VLAN is enabled, all unauthorized ports automatically join the VLAN selected in the *Guest VLAN ID* field. If a port is later authorized, it is removed from the guest VLAN.
- **Guest VLAN ID**—Select the guest VLAN from the list of VLANs.
- **Guest VLAN Timeout**—Define a time period:
  - After linkup, if the software does not detect the 802.1X supplicant, or the authentication has failed, the port is added to the guest VLAN, only after the *Guest VLAN timeout* period has expired.

  - If the port state changes from *Authorized* to *Not Authorized*, the port is added to the guest VLAN only after the *Guest VLAN* timeout has expired.

- Traps—To enable traps, select one of more of the following options:
  - *802.1x Authentication Failure Traps*—Select to generate a trap if 802.1x authentication fails.
  - *802.1x Authentication Success Traps*—Select to generate a trap if 802.1x authentication succeeds.
  - *MAC Authentication Failure Traps*—Select to generate a trap if MAC authentication fails.
  - *MAC Authentication Success Traps*—Select to generate a trap if MAC authentication succeeds.
- When the switch is in Layer 2 switch mode:
  - *Web Authentication Failure Traps*—Select to generate a trap if Web authentication fails.
  - *Web Authentication Success Traps*—Select to generate a trap if Web authentication succeeds.
  - *Web Authentication Quiet Traps*—Select to generate a trap if a quiet period commences.

When the device is in Layer 3 router mode, the VLAN Authentication Table displays all VLANs, and indicates whether authentication has been enabled on them.

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

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/MAC/Web Authentication > **Port Authentication.**

This page displays authentication settings for all ports.

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

STEP 3 Enter the parameters.

- **Interface**—Select a port.
- **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 device does not provide authentication services to the client through the interface.
  - *Auto*—Enables port-based authentication and authorization on the device. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.
  - *Force Authorized*—Authorizes the interface without authentication.
- **RADIUS VLAN Assignment**—Select to enable Dynamic VLAN assignment on the selected port.
  - *Disable*—Feature is not enabled.
  - *Reject*—If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN, the supplicant is rejected.
  - *Static*—If the RADIUS server authorized the supplicant, but did not provide a supplicant VLAN, the supplicant is accepted.
- **Guest VLAN**—Select to indicate that the usage of a previously-defined guest VLAN is enabled for the device. The options are:
  - *Selected*—Enables using a guest VLAN for unauthorized ports. If a guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the Guest VLAN ID field in the 802.1X Port Authentication page.

After an authentication failure, and if guest VLAN is activated globally on a given port, the guest VLAN is automatically assigned to the unauthorized ports as an Untagged VLAN.

  - *Cleared*—Disables guest VLAN on the port.

- **802.1X Based Authentication**—802.1X authentication is the only authentication method performed on the port.
- **MAC Based Authentication**—Port is authenticated based on the supplicant MAC address. Only 8 MAC-based authentications can be used on the port.

  NOTE For MAC authentication to succeed, the RADIUS server supplicant username and password must be the supplicant MAC address. The MAC address must be in lower case letters and entered without the . or - separators; for example: 0020aa00bbcc.

- **Web Based Authentication**—This is only available in Layer 2 switch mode. Select to enable web-based authentication on the switch.
- **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:
  - *Initialize*—In process of coming up.
  - *Force-Authorized*—Controlled port state is set to Force-Authorized (forward traffic).
  - *Force-Unauthorized*—Controlled port state is set to Force-Unauthorized (discard traffic).

  NOTE If the port is not in Force-Authorized or Force-Unauthorized, it is in Auto Mode and the authenticator displays the state of the authentication in progress. After the port is authenticated, the state is shown as Authenticated.

- **Time Range**—Enable a limit on the time that the specific port is authorized for use if 802.1x has been enabled (Port -Based authentication is checked).
- **Time Range Name**—Select the profile that specifies the time range.

- **Maximum WBA Login Attempts—**Available only in Layer 2 switch mode. Enter the maximum number of login attempts allowed on the interface. Select either **Infinite** for no limit or **User Defined** to set a limit.
- **Max WBA Silence Period—**Available only in Layer 2 switch mode. Enter the maximum length of the silent period allowed on the interface. Select either **Infinite** for no limit or **User Defined** to set a limit.
- **Max Hosts—**Enter the maximum number of authorized hosts allowed on the interface. Select either **Infinite** for no limit or **User Defined** to set a limit.

  NOTE Set this value to 1 to simulate single-host mode for web-based authentication in multi-sessions mode.
- **Quiet Period—**Enter the number of seconds that the device remains in the quiet state following a failed authentication exchange.
- **Resending EAP—**Enter the number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request.
- **Max EAP Requests—**Enter the maximum number of EAP requests that 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 device resends a request to the authentication server.

STEP 4 Click **Apply**. The port settings are written to the Running Configuration file.

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.

See **Port Host Modes** for an explanation of these modes.

To define 802.1X advanced settings for ports:

STEP 1 Click **Security** > 802.1X/MAC/Web Authentication > **Host and Session Authentication**.

802.1X authentication parameters are described for all ports. All fields except the following are described in the Edit Host and Session Authentication page.

- **Number of Single Host 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.**

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 **Port Host Modes**.

  The following fields are only relevant if you select Single in the Host Authentication field.

Single Host Violation Settings:

- **Action on Violation**—Select the action to be applied to packets arriving in Single Session/Single Host mode, from a host whose MAC address is not the supplicant MAC address. The options are:
  - *Protect (Discard)*—Discards the packets.
  - *Restrict (Forward)*—Forwards the packets.
  - *Shutdown*—Discards the packets and shuts down the port. The ports remains shut down until reactivated, or until the device is rebooted.
- **Traps** (on single host violation)—Select to enable traps.
- **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.
- **Number of Violations**—Displays the number violations (number of packets in Single Session/Single Host mode, from a host whose MAC address is not the supplicant MAC address).

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

Viewing Authenticated Hosts

To view details about authenticated users:

STEP 1 Click **Security** > 802.1X/MAC/Web Authentication > **Authenticated Hosts.**

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.
- **Authentication Server**—RADIUS server.
- **MAC Address**—Displays the supplicant MAC address.
- **VLAN ID**—Port's VLAN.

Locked Clients

To view clients who have been locked out because of failed login attempts and to unlock a locked client:

STEP 1 Click **Security** > **802.1X/MAC/Web Authentication** > **Locked Client**.

The following fields are displayed:

- **Interface**—Port that is locked.
- **MAC Address**—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*.
- **Remaining Time(Sec)**—The time remaining for the port to be locked.

STEP 2 Select a port.

STEP 3 Click Unlock.

Web Authentication Customization

This page enables designing web-based authentication pages in various languages.

You can add up to 4 languages.

NOTE Up to 5 HTTP users and one HTTPS user can request web-based authentication at the same time. When these users are authenticated, more users can request authentication.

To add a language for web-based authentication:

STEP 1 Click **Security** > **802.1X/MAC/Web Authentication** > **Web Authentication Customization.**

STEP 2 Click **Add.**

STEP 3 Select a language from the **Language** drop-down list.

STEP 4 Select **Set as Default Display Language** if this language is the default language. the default language pages are displayed if the end user does not select a language.

STEP 5 Click **Apply** and the settings are saved to the Running Configuration file.

To customize the web-authentication pages:

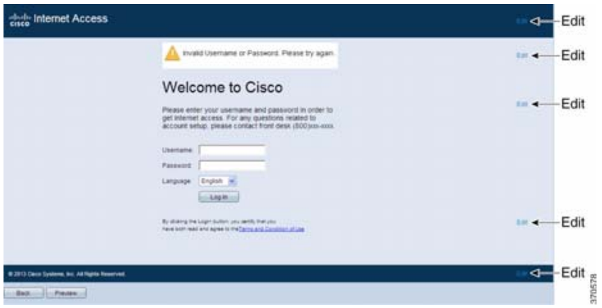
STEP 1 Click **Security** > **802.1X/MAC/Web Authentication** > **Web Authentication Customization.**

This page displays the languages that can be customized.

STEP 2 Click **Edit Logon Page**.

Figure 4 The following page is displayed:

.



Invalid Username or Password. Please try again.

Welcome to Cisco

Please enter your username and password in order to get internet access. For any questions related to account setup, please contact front desk (800)xxx-xxxx.

STEP 3 Click **Edit1**. The following fields are displayed:

- **Language**—Displays the page's language.
- **Color Scheme**—Select one of the contrast options.

  If the **Custom** color scheme is selected, the following options are available:

  - *Page Background Color*—Enter the ASCII code of the background color. The selected color is shown in the Text field.
  - *Header and Footer Background Color*—Enter the ASCII code of the header and footer background color. The selected color is shown in the Text field.
  - *Header and Footer Text Color*—Enter the ASCII code of the header and footer text color. The selected color is shown in the Text field.
  - *Hyperlink Color*—Enter the ASCII code of the hyperlink color. The selected color is shown in the Text field.
- **Current Logo Image**—Select one of the following options:

- *None*—No logo.
- *Default*—Use the default logo.
- *Other*—Select to enter a customized logo.

If the **Other** logo option is selected, the following options are available:

- *Logo Image Filename*—Enter the logo file name or **Browse** to the image.
- *Application Text*—Enter text to accompany the logo.
- *Window Title Text*—Enter a title for the Login page.

STEP 4 Click **Apply** and the settings are saved to the Running Configuration file.

STEP 5 Click **Edit2**. The following fields are displayed:

- **Invalid User Credentials**—Enter the text of the message to be displayed when the end user enters an invalid username or password.
- **Service Not Available**—Enter the text of the message to be displayed when the authentication service is not available.

STEP 6 Click **Apply** and the settings are saved to the Running Configuration file.

STEP 7 Click **Edit3**. The following fields are displayed:

- **Welcome Message**—Enter the text of the message to be displayed when the end user logs on.
- **Instructional Message**—Enter the instructions to be displayed to the end user.
- **RADIUS Authentication**—Displays whether RADIUS authentication is enabled. If so, the username and password must be included in the login page.
- **Username Textbox**—Select for a username textbox to be displayed.
- **Username Textbox Label**—Select the label to be displayed before the username textbox.
- **Password Textbox**—Select for a password textbox to be displayed.
- **Password Textbox Label**—Select the label to be displayed before the password textbox.
- **Language Selection**—Select to enable the end user to select a language.

- **Language Dropdown Label**—Enter the label of the language selection dropdown.
- **Login Button Label**—Enter the label of the login button.
- **Login Progress Label**—Enter the text that will be displayed during the login process.

STEP 8 Click **Apply** and the settings are saved to the Running Configuration file.

STEP 9 Click **Edit4**. The following fields are displayed:

- **Terms and Conditions**—Select to enable a terms and conditions text box.
- **Terms and Conditions Warning**—Enter the text of the message to be displayed as instructions to enter the terms and conditions.
- **Terms and Conditions Contents**—Enter the text of the message to be displayed as terms and conditions.

STEP 10 Click **Apply** and the settings are saved to the Running Configuration file.

STEP 11 **Edit5**. The following fields are displayed:

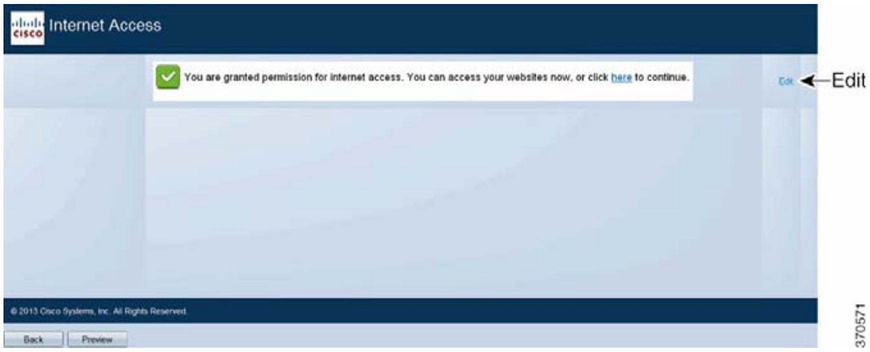
- **Copyright**—Select to enable displaying copyright text.
- **Copyright Text**—Enter the copyright text.

STEP 12 Click **Apply** and the settings are saved to the Running Configuration file.

STEP 13 Click **Edit Success Page**.

Figure 5 The following page is displayed

.



You are granted permission for internet access. You can access your websites now, or click here to continue.

STEP 14 Click the **Edit.** button on the right side of the page.

STEP 15 Enter the **Success Message**, which is the text that will be displayed if the end user successfully logs in.

STEP 16 Click **Apply** and the settings are saved to the Running Configuration file.

To preview the login or success message, click **Preview**.

To set one of the languages as the default language, click **Set Default Display Language**.

Defining Time Ranges

See **<300-500>Time Range** for an explanation of this feature.

Authentication Method and Port Mode Support

The following table shows which combinations of authentication method and port mode are supported.

Authentication Method	Single-host	Multi-host	Multi-sessions	
			Device in L3	Device in L2
802.1x	†	†	†	†
MAC	†	†	†	†
WEB	N/S	N/S	N/S	†

Legend:

†—The port mode also supports the guest VLAN and RADIUS-VLAN assignment.

N/S—The authentication method does not support the port mode.

NOTE Web-based authentication requires TCAM support for input traffic classification and can be supported only by the full multi-sessions mode. You can simulate the single-host mode by setting Max Hosts parameter to 1 in the Port Authentication page.

Mode Behavior

The following table describes how authenticated and non-authenticated traffic is handled in various situations.

	Unauthenticated Traffic				Authenticated Traffic			
	With Guest VLAN		Without Guest VLAN		With Radius VLAN		Without Radius VLAN	
	Untagged	Tagged	Untagged	Tagged	Untagged	Tagged	Untagged	Tagged
Single-host	Frames are re-mapped to the guest VLAN	Frames are dropped unless they belong to the guest VLAN or to the unauthenticated VLANs	Frames are dropped	Frames are dropped unless they belong to the unauthenticated VLANs	Frames are re-mapped to the RADIUS assigned VLAN	Frames are dropped unless they belong to the RADIUS VLAN or to the unauthenticated VLANs	Frames are bridged based on the static VLAN configuration	Frames are bridged based on the static VLAN configuration
Multi-host	Frames are re-mapped to the guest VLAN	Frames are dropped unless they belongs to the guest VLAN or to the unauthenticated VLANs	Frames are dropped	Frames are dropped unless they belongs to the unauthenticated VLANs	Frames are re-mapped to the Radius assigned VLAN	Frames are dropped unless they belongs to the Radius VLAN or to the unauthenticated VLANs	Frames are bridged based on the static VLAN configuration	Frames are bridged based on the static VLAN configuration
Lite multi-sessions	N/S	N/S	Frames are dropped	Frames are dropped unless they belongs to the unauthenticated VLANs	N/S	N/S	Frames are bridged based on the static VLAN configuration	Frames are bridged based on the static VLAN configuration

	Unauthenticated Traffic				Authenticated Traffic			
	With Guest VLAN		**Without Guest VLAN**		**With Radius VLAN**		**Without Radius VLAN**	
	Untagged	**Tagged**	**Untagged**	**Tagged**	**Untagged**	**Tagged**	**Untagged**	**Tagged**
Full multi-sessions	Frames are re-mapped to the guest VLAN	Frames are re-mapped to the guest VLAN unless they belongs to the unauthenticated VLANs	Frames are dropped	Frames are dropped unless they belongs to the unauthenticated VLANs	Frames are re-mapped to the RADIUS assigned VLAN	Frames are re-mapped to the Radius VLAN unless they belongs to the unauthenticated VLANs	Frames are bridged based on the static VLAN configuration	Frames are bridged based on the static VLAN configuration

20

Security: IPV6 First Hop Security

This section describes how First Hop Security (FHS) works and how to configure it in the GUI.

It covers the following topics:

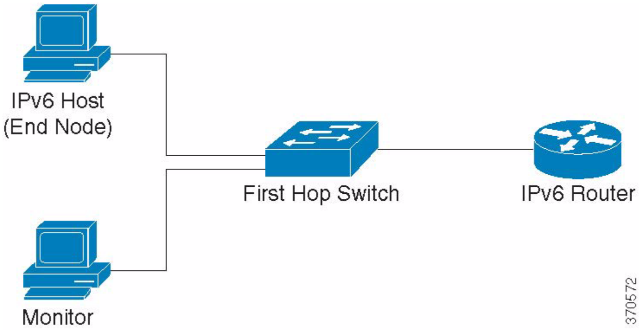
- **First Hop Security Overview**
- **Router Advertisement Guard**
- **Neighbor Discovery Inspection**
- **DHCPv6 Guard**
- **Neighbor Binding Integrity**
- **Attack Protection**
- **Policies, Global Parameters and System Defaults**
- **Common Tasks**
- **Default Settings and Configuration**
- **Default Settings and Configuration**
- **Configuring First Hop Security through Web GUI**

First Hop Security Overview

IPv6 FHS is a suite of features designed to secure link operations in an IPv6-enabled network. It is based on the Neighbor Discovery Protocol and DHCPv6 messages.

In this feature, a Layer 2 switch (as shown in **Figure 6**) filters Neighbor Discovery Protocol messages, DHCPv6 messages and user data messages according to a number of different rules.

Figure 6 First Hop Security Configuration



A separate and independent instance of IPv6 First Hop Security runs on each VLAN on which the feature is enabled.

Abbreviations

Name	Description
CPA message	Certification Path Advertisement message
CPS message	Certification Path Solicitation message
DAD-NS message	Duplicate Address Detection Neighbor Solicitation message
FCFS-SAVI	First Come First Served - Source Address Validation Improvement

Name	Description
NA message	Neighbor Advertisement message
NDP	Neighbor Discovery Protocol
NS message	Neighbor Solicitation message
RA message	Router Advertisement message
RS message	Router Solicitation message
SAVI	Source Address Validation Improvement

IPv6 First Hop Security Components

IPv6 First Hop Security includes the following features:

- IPv6 First Hop Security Common
- RA Guard
- ND Inspection
- Neighbor Binding Integrity
- DHCPv6 Guard

These components can be enabled or disabled on VLANs.

There are two empty, pre-defined policies per each feature with the following names: vlan_default and port_default. The first one is attached to each VLAN that is not attached to a user-defined policy and the second one is connected to each interface and VLAN that is not attached to a user-defined policy. These policies cannot be attached explicitly by the user. See **Policies, Global Parameters and System Defaults**.

IPv6 First Hop Security Pipe

If IPv6 First Hop Security is enabled on a VLAN, the switch traps the following messages:

- Router Advertisement (RA) messages
- Router Solicitation (RS) messages
- Neighbor Advertisement (NA) messages

- Neighbor Solicitation (NS) messages
- ICMPv6 Redirect messages
- Certification Path Advertisement (CPA) messages
- Certification Path Solicitation (CPS) messages
- DHCPv6 messages

Trapped RA, CPA, and ICMPv6 Redirect messages are passed to the RA Guard feature. RA Guard validates these messages, drops illegal message, and legal messages passes to the ND Inspection feature.

ND Inspection validates these messages and drops illegal message, and legal messages passes to the IPv6 Source Guard feature.

Trapped DHCPv6 messages are passed to the DHCPv6 Guard feature. DHCPv6 Guard validates these messages, drops illegal message, and legal messages passes to the IPv6 Source Guard feature.

Trapped data messages are passed to the IPv6 Source Guard feature. IPv6 Source Guard validates received messages (trapped data messages, NDP messages from ND Inspection, and DHCPv6 messages from DHCPv6 Guard) using the Neighbor Binding Table, drops illegal messages, and passes legal messages to forwarding.

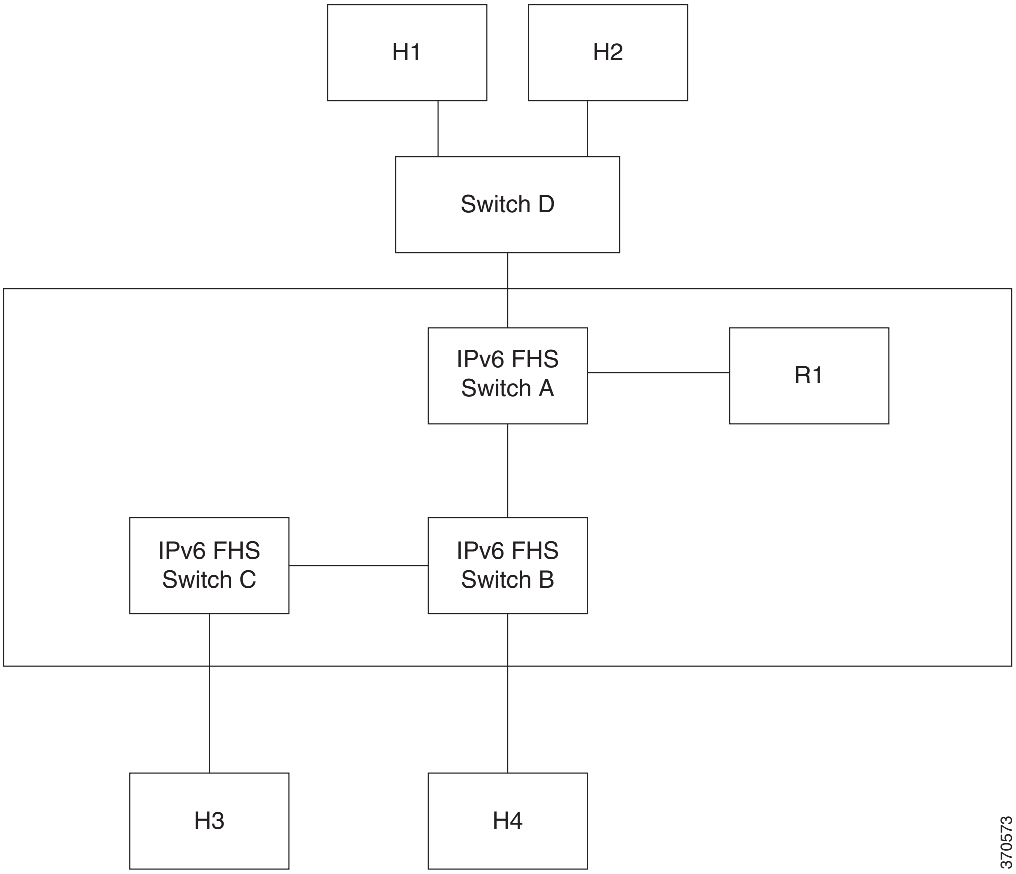
Neighbor Binding Integrity learns neighbors from the received messages (NDP and DHCPv6 messages) and stores them in the Neighbor Binding table. Additionally, static entries can be added manually. After learning the addresses, the NBI feature passes the frames for forwarding.

Trapped RS,CPS NS and NA messages are also passed to the ND Inspection feature. ND Inspection validates these messages, drops illegal messages, and passes legal messages to the IPv6 Source Guard feature.

IPv6 First Hop Security Perimeter

IPv6 First Hop Security switches can form a perimeter separating untrusted area from trusted area. All switches inside the perimeter support IPv6 First Hop Security, and hosts and routers inside this perimeter are trusted devices. For example, the links SwitchC-H3, SwitchB-H4, and SwitchA-SwitchD on **Figure 7** form the perimeter, while links SwitchA-SwitchB, SwitchB-SwitchC, and SwitchA-R1 are inner links inside the protected area.

Figure 7 IPv6 First Hop Security Perimeter



The **device-role** command in the Neighbor Binding policy configuration screen specifies the perimeter.

Each IPv6 First Hop Security switch establishes binding for neighbors partitioned by the edge. In this way, binding entries are distributed on IPv6 First Hop Security devices forming the perimeter. The IPv6 First Hop Security devices can then provide binding integrity to the inside of the perimeter, without setting up bindings for all the addresses on each device.

Router Advertisement Guard

Router Advertisement (RA) Guard is the first FHS feature that treats trapped RA messages. RA Guard supports the following functions:

- Filtering of received RA, CPA, and ICMPv6 redirect messages.
- Validation of received RA messages.

Filtering of Received RA, CPA, and IPCMv6 redirect Messages

RA Guard discards RA and CPA messages received on interfaces whose role are not router. The interface role is configured in the Security > IPv6 First Hop Security > RA Guard Settings page.

Validation of RA messages

RA Guard validates RA messages using the filtering based on the RA Guard policy attached to the interface. These policies can be configured in the RA Guard Settings page.

If a message does not pass verification, it is dropped. If the logging packet drop configuration on the FHS common component is enabled, a rate limited SYSLOG message is sent.

Neighbor Discovery Inspection

Neighbor Discovery (ND) Inspection supports the following functions:

- Validation of received Neighbor Discovery protocol messages.
- Egress filtering

Message Validation

ND Inspection validates the Neighbor Discovery protocol messages, based on an ND Inspection policy attached to the interface. This policy can be defined in the ND Inspection Settings page.

If a message does not pass the verification defined in the policy, it is dropped and a rate limited SYSLOG message is sent.

Egress Filtering

ND Inspection blocks forwarding of RS and CPS messages on interfaces configured as host interfaces.

DHCPv6 Guard

DHCPv6 Guard treats the trapped DHCPv6 messages. DHCPv6 Guard supports the following functions:

- Filtering of received DHCPv6 messages.

  DHCP Guard discards DHCPv6 reply messages received on interfaces whose role is client. The interface role is configured in the DHCP Guard Settings page.

- Validation of received DHCPv6 messages.

  DHCPv6 Guard validates DHCPv6 messages that match the filtering based on the DHCPv6 Guard policy attached to the interface.

If a message does not pass verification, it is dropped. If the logging packet drop configuration on the FHS common component is enabled, a rate limited SYSLOG message is sent.

Neighbor Binding Integrity

Neighbor Binding (NB) Integrity establishes binding of neighbors.

A separate, independent instance of NB Integrity runs on each VLAN on which the feature is enabled.

Learning Advertised IPv6 Prefixes

NB Integrity learns IPv6 prefixes advertised in RA messages and saves it in the Neighbor Prefix table. The prefixes are used for verification of assigned global IPv6 addresses.

By default, this validation is disabled. When it is enabled, addresses are validated against the prefixes in the Neighbor Binding Settings page.

Static prefixes used for the address validation can be added in the Neighbor Binding Table page.

Neighbor Binding Table Overflow

When there is no free space to create a new entry, the new entry overrides the entry with the highest creation time.

Establishing Binding of Neighbors

An IPv6 First Hop Security switch can discover and record binding information by using the following methods:

- **NBI-NDP Method**: Learning IPv6 addresses from the snooped Neighbor Discovery Protocol messages
- **NBI-Manual Method:** By manual configuration

An IPv6 address is bound to a link layer property of the host's network attachment. This property, called a "binding anchor" consists of the interface identifier (ifIndex) through which the host is connected to and the host’s MAC address.

IPv6 First Hop Security switch establishes binding only on perimeterical interfaces (see **IPv6 First Hop Security Perimeter**).

Binding information is saved in the Neighbor Binding table.

NBI-NDP method

The NBI-NDP method used is based on the FCFS- SAVI method specified in RFC6620, with the following differences:

- Unlike FCFS-SAVI, which supports only binding for link local IPv6 addresses, NBI-NDP additionally supports binding global IPv6 addresses as well.
- NBI-NDP supports IPv6 address binding only for IPv6 addresses learnt from NDP messages. Source address validation for data message is provided by IPv6 Source Address Guard.
- In NBI-NDP, proof of address ownership is based on the First-Come, First-Served principle. The first host that claims a given source address is the owner of that address until further notice. Since no host changes are acceptable, a way must be found to confirm address ownership without requiring a new protocol. For this reason, whenever an IPv6 address is first learned from an NDP message, the switch binds the address to the interface. Subsequent NDP messages containing this IPV6 address can be checked against the same binding anchor to confirm that the originator owns the source IP address.

  The exception to this rule occurs when an IPv6 host roams in the L2 domain or changes its MAC address. In this case, the host is still the owner of the IP address, but the associated binding anchor might have changed. To cope with this case, the defined NBI-NDP behavior implies verification of whether or not the host is still reachable by sending DAD-NS messages to the previous binding interface. If the host is no longer reachable at the previously-recorded binding anchor, NBI-NDP assumes that the new anchor is valid and changes the binding anchor. If the host is still reachable using the previously recorded binding anchor, the binding interface is not changed.

To reduce the size of the Neighbor Binding table, NBI-NDP establishes binding only on perimeterical interfaces (see IPv6 First Hop Security Perimeter) and distributes binding information through internal interfaces using NS and NA messages. Before creating an NBI-NDP local binding, the device sends a DAD-NS message querying for the address involved. If a host replies to that message with an NA message, the device that sent the DAD-NS message infers that a binding for that address exists in another device and does not create a local binding for it. If no NA message is received as a reply to the DAD-NS message, the local device infers that no binding for that address exists in other devices and creates the local binding for that address.

NBI-NDP supports a lifetime timer. A value of the timer is configurable in the Neighbor Binding Settings page. The timer is restarted each time that the bound IPv6 address is confirmed. If the timer expires, the device sends up to 2 DAD-NS messages with short intervals to validate the neighbor.

NB Integrity Policy

In the same way that other IPv6 First Hop Security features function, NB Integrity behavior on a interface is specified by an NB Integrity policy attached to an interface. These policies are configured in the Neighbor Binding Settings page.

Attack Protection

The section describes attack protection provided by IPv6 First Hop Security

Protection against IPv6 Router Spoofing

An IPv6 host can use the received RA messages for:

- IPv6 router discovery
- Stateless address configuration

A malicious host could send RA messages advertising itself as an IPv6 router and providing counterfeit prefixes for stateless address configuration.

RA Guard provides protection against such attacks by configuring the interface role as a host interface for all interfaces where IPv6 routers cannot be connected.

Protection against IPv6 Address Resolution Spoofing

A malicious host could send NA messages advertising itself as an IPv6 Host having the given IPv6 address.

NB Integrity provides protection against such attacks in the following ways:

- If the given IPv6 address is unknown, the Neighbor Solicitation (NS) message is forwarded only on inner interfaces.
- If the given IPv6 address is known, the NS message is forwarded only on the interface to which the IPv6 address is bound.

- A Neighbor Advertisement (NA) message is dropped if the target IPv6 address is bound with another interface.

Protection against IPv6 Duplication Address Detection Spoofing

An IPv6 host must perform Duplication Address Detection for each assigned IPv6 address by sending a special NS message (Duplicate Address Detection Neighbor Solicitation message (DAD_NS) message).

A malicious host could send reply to a DAD_RS message advertising itself as an IPv6 host having the given IPv6 address.

NB Integrity provides protection against such attacks in the following ways:

- If the given IPv6 address is unknown, the DAD_NS message is forwarded only on inner interfaces.
- If the given IPv6 address is known, the DAD_NS message is forwarded only on the interface where the IPv6 address is bound.
- An NA message is dropped if the target IPv6 address is bound with another interface.

Protection against DHCPv6 Server Spoofing

An IPv6 host can use the DHCPv6 protocol for:

- Stateless Information configuration
- Statefull address configuration

A malicious host could send DHCPv6 reply messages advertising itself as a DHCPv6 server and providing counterfeit stateless information and IPv6 addresses. DHCPv6 Guard provides protection against such attacks by configuring the interface role as a client port for all ports to which DHCPv6 servers cannot be connected.

Protection Against NBD Cache Spoofing

An IPv6 router supports the Neighbor Discovery Protocol (NDP) cache that maps the IPv6 address to the MAC address for the last hop routing.

A malicious host could send IPv6 messages with a different destination IPv6 address for the last hop forwarding, causing overflow of the NBD cache.

An embedded mechanism in the NDP implementation, which limits the number of entries allowed in the INCOMPLETE state in the Neighbor Discovery cache, provides protection.

Policies, Global Parameters and System Defaults

Each feature of FHS can be enabled or disabled individually. No feature is enabled by default.

Features must initially be enabled on specific VLANs. When you enable the feature, you can also define global configuration values for that feature’s rules of verification. If you do not define a policy that contain different values for these verification rules, the global values are used to apply the feature to packets.

Policies

Policies contain the rules of verification that are performed on input packets. They can be attached to VLANs and also to ports and LAGs. If the feature is not enabled on a VLAN, the policies have no effect.

Policies can be user-defined or default policies (see below).

Default Policies

Empty default polices exist for each FHS feature and are by default attached to all VLANs and interfaces. The default policies are named: "vlan_default" and "port_default" (for each feature):

- Rules can be added to these default policies. You cannot manually attach default policies to interfaces. They are attached by default.
- Default policies can never be deleted. You can only delete the user-added configuration.

User-Defined Policies

You can define policies other than the default policies.

When a user-defined policy is attached to an interface, the default policy for that interface is detached. If the user-define policy is detached from the interface, the default policy is reattached.

Policies do not take effect until:

- The feature in the policy is enabled on the VLAN containing the interface
- The policy is attached to the interface (VLAN, port or LAG).

When you attach a policy, the default policy for that interface is detached. When you remove the policy from the interface, the default policy is reattached.

You can only attach 1 policy (for a specific feature) to a VLAN.

You can attach multiple policies (for a specific feature) to an interface if they specify different VLANs.

Levels of Verification Rules

The final set of rules that is applied to an input packet on an interface is built in the following way:

- The rules configured in policies attached to the interface (port or LAG) on which the packet arrived are added to the set.
- The rules configured in the policy attached to the VLAN are added to the set if they have not been added at the port level.
- The global rules are added to the set if they have not been added at the VLAN or port level.

Rules defined at the port level override the rules set at the VLAN level. Rules defined at the VLAN level override the globally-configured rules. The globally-configured rules override system defaults.

Common Tasks

First Hop Security Common Work Flow

STEP 1 In the FHS Settings page, enter the list of VLANs on which this feature is enabled.

STEP 2 In this same page, set the Global Packet Drop Logging feature.

STEP 3 If required, either configure a user-defined policy or add rules to the default policies for the feature.

STEP 4 Attach the policy to a VLAN, port or LAG using either the Policy Attachment (VLAN) or Policy Attachment (Port) pages.

Router Advertisement Guard Work Flow

STEP 1 In the RA Guard Settings page, enter the list of VLANs on which this feature is enabled.

STEP 2 In this same page, set the global configuration values that are used if no values are set in a policy.

STEP 3 If required, either configure a user-defined policy or add rules to the default policies for the feature.

STEP 4 Attach the policy to a VLAN, port or LAG using either the Policy Attachment (VLAN) or Policy Attachment (Port) pages.

DHCPv6 Guard Work Flow

STEP 1 In the DHCPv6 Guard Settings page, enter the list of VLANs on which this feature is enabled.

STEP 2 In this same page, set the global configuration values that are used if no values are set in a policy.

STEP 3 If required, either configure a user-defined policy or add rules to the default policies for the feature.

STEP 4 Attach the policy to a VLAN, port or LAG using either the Policy Attachment (VLAN) or Policy Attachment (Port) pages.

Neighbor Discovery Inspection Work Flow

STEP 1 In the ND Inspection Settings page, enter the list of VLANs on which this feature is enabled.

STEP 2 In this same page, set the global configuration values that are used if no values are set in a policy.

STEP 3 If required, either configure a user-defined policy or add rules to the default policies for the feature.

STEP 4 Attach the policy to a VLAN, port or LAG using either the Policy Attachment (VLAN) or Policy Attachment (Port) pages.

Neighbor Binding Work Flow

STEP 1 In the Neighbor Bindings Settings page, enter the list of VLANs on which this feature is enabled.

STEP 2 In this same page, set the global configuration values that are used if no values are set in a policy.

STEP 3 If required, either configure a user-defined policy or add rules the default policies for the feature.

STEP 4 Add any manual entries required in the Neighbor Binding Table page

STEP 5 Attach the policy to a VLAN, port or LAG using either the Policy Attachment (VLAN) or Policy Attachment (Port) pages.

Default Settings and Configuration

If IPv6 First Hop Security is enabled on a VLAN, the switch traps the following messages by default:

- Router Advertisement (RA) messages
- Router Solicitation (RS) messages
- Neighbor Advertisement (NA) messages
- Neighbor Solicitation (NS) messages
- ICMPv6 Redirect messages
- Certification Path Advertisement (CPA) messages
- Certification Path Solicitation (CPS) message
- DHCPv6 messages

The FHS features are disabled by default.

Before You Start

No preliminary tasks are required.

Configuring First Hop Security through Web GUI

FHS Common Settings

Use the FHS Settings page to enable the FHS Common feature on a specified group of VLANs and to set the global configuration value for logging packet dropping. If required, a policy can be added or the packet drop logging can be added to the system-defined default policy.

To configure First Hop Security Common on ports or LAGs:

STEP 1 Click **Security** > **First Hop Security** > **FHS Settings**.

STEP 2 Enter the following global configuration fields:

- **FHS VLAN List**—Enter one or more VLANs on which First Hop Security is enabled.
- **Packet Dropped Logging**—Select to create a SYSLOG when a packet is dropped by a First Hop Security feature. This is the global default value if no policy is defined.

STEP 3 Create a FHS policy if required by clicking **Add**.

Enter the following fields:

- **Policy Name**—Enter a user-defined policy name.
- **Packet Drop Logging**—Select to create a SYSLOG when a packet is dropped as a result of a First Hop Security feature within this policy.
  - *Inherit*—Use the value from the VLAN or the global configuration.
  - *Enable*—Create a SYSLOG when a packet is dropped as a result of First Hop Security.
  - *Disable*—Do not create a SYSLOG when a packet is dropped as a result of First Hop Security.

RA Guard Settings

Use the RA Guard Settings page to enable the RA Guard feature on a specified group of VLANs and to set the global configuration values for this feature. If required, a policy can be added or the system-defined default RA Guard policies can be configured in this page.

To configure RA Guard on ports or LAGs:

STEP 1 Click **Security** > **First Hop Security** > **RA Guard Settings**.

STEP 2 Enter the following global configuration fields:

- **RA Guard VLAN List—**Enter one or more VLANs on which RA Guard is enabled.
- **Minimal Hop Limit—**This field indicates whether the RA Guard policy will check the minimum hop limit of the packet received.
  - *Minimal Hop Limit*—Verifies that the hop-count limit is greater than or equal to this value.
  - *No Verification*—Disables verification of the lower boundary of the hop count limit.
- **Maximal Hop Limit**—This field indicates whether the RA Guard policy will check the maximum hop limit of the packet received.
  - *Maximal Hop Limit*—Verifies that the hop-count limit is less than or equal to this value. The value of the high boundary must be equal or greater than the value of the low boundary.
  - *No Verification*—Disables verification of the high boundary of the hop-count limit.
- **Managed Configuration Flag—**This field specifies verification of the advertised Managed Address Configuration flag within an IPv6 RA Guard policy.
  - *No Verification*—Disables verification of the advertised Managed Address Configuration flag.
  - *On*—Enables verification of the advertised Managed Address Configuration flag.
  - *Off*—The value of the flag must be 0.

- **Other Configuration Flag—**This field specifies verification of the advertised Other Configuration flag within an IPv6 RA Guard policy.
  - *No Verification*—Disables verification of the advertised Other Configuration flag.
  - *On*—Enables verification of the advertised Managed Other flag.
  - *Off*—The value of the flag must be 0.
- **Minimal Route Preference—**This field indicates whether the RA Guard policy will verify the minimum advertised Default Router Preference value in RA messages within an RA Guard policy.
  - *No Verification*—Disables verification of the low boundary of Advertised Default Router Preference.
  - *Low*—Specifies the minimum allowed Advertised Default Router Preference value. The following values are acceptable: low, medium and high (see RFC4191).
  - *Medium*—Specifies the minimum allowed Advertised Default Router Preference value. The following values are acceptable: low, medium and high (see RFC4191).
  - *High*—Specifies the minimum allowed Advertised Default Router Preference value. The following values are acceptable: low, medium and high (see RFC4191).
- **Maximal Route Preference—**This field indicates whether the RA Guard policy will verify the maximum advertised Default Router Preference value in RA messages within an RA Guard policy.
  - *No Verification*—Disables verification of the high boundary of Advertised Default Router Preference.
  - *Low*—Specifies the maximum allowed Advertised Default Router Preference value. The following values are acceptable: low, medium and high (see RFC4191).
  - *Medium*—Specifies the maximum allowed Advertised Default Router Preference value. The following values are acceptable: low, medium and high (see RFC4191).
  - *High*—Specifies the maximum allowed Advertised Default Router Preference value. The following values are acceptable: low, medium and high (see RFC4191).

To create an RA Guard policy or to configure the system-defined default policies, click **Add** and enter the above parameters.

If required, click either **Attach Policy to VLAN** or **Attach Policy to Interface**.

DHCPv6 Guard Settings

Use the DHCPv6 Guard Settings page to enable the DHCPv6 Guard feature on a specified group of VLANs and to set the global configuration values for this feature. If required, a policy can be added or the system-defined default DHCPv6 Guard policies can be configured in this page.

To configure DHCPv6 Guard on ports or LAGs:

STEP 1 Click **Security** > **First Hop Security** > **DHCPv6 Guard Settings**.

STEP 2 Enter the following global configuration fields:

- **DHCPv6 Guard VLAN List—**Enter one or more VLANs on which DHCPv6 Guard is enabled.
- **Minimal Preference—**This field indicates whether the DHCPv6 Guard policy will check the minimum advertised preference value of the packet received.
  - *No Verification*—Disables verification of the minimum advertised preference value of the packet received.
  - *User Defined*—Verifies that the advertised preference value is greater than or equal to this value. This value must be less than the Maximal Preference value.
- **Maximal Preference—**This field indicates whether the DHCPv6 Guard policy will check the maximum advertised preference value of the packet received. This value must be greater than the Minimal Preference value.
  - *No Verification*—Disables verification of the lower boundary of the hop count limit.
  - *User Defined*—Verifies that the advertised preference value is less than or equal to this value.

STEP 3 If required, click **Add** to create a DHCPv6 policy.

STEP 4 Enter the following fields:

- **Policy Name—**Enter a user-defined policy name.

- **Device Role**—Select either **Server** or **Client** to specify the role of the device attached to the port for DHCPv6 Guard.
  - *Inherited*—Role of device is inherited from either the VLAN or system default (client).
  - *Client*—Role of device is client.
  - *Host*—Role of device is host.
- **Match Reply Prefixes**—Select to enable verification of the advertised prefixes in received DHCP reply messages within a DHCPv6 Guard policy.
  - *Inherited*—Value is inherited from either the VLAN or system default (no verification).
  - *No Verification*—Advertised prefixes are not verified.
  - *Match List*— IPv6 prefix list to be matched.
- **Match Server Address**—Select to enable verification of the DHCP server's and relay's IPv6 address in received DHCP reply messages within a DHCPv6 Guard policy.
  - *Inherited*—Value is inherited from either the VLAN or system default (no verification).
  - *No Verification*—Disables verification of the DHCP server's and relay's IPv6 address.
  - *Match List*— IPv6 prefix list to be matched.
- **Minimal Preference**—See above.
- **Maximal Preference**—See above.

STEP 5 If required, click either **Attach Policy to VLAN** or **Attach Policy to Interface**.

Neighbor Discovery Inspection Settings

Use the ND Inspection Settings page to enable the ND Inspection feature on a specified group of VLANs and to set the global configuration values for this feature. If required, a policy can be added or the system-defined default ND Inspection policies can be configured in this page.

To configure ND Inspection on ports or LAGs:

STEP 1 Click **Security** > **First Hop Security** > **ND Inspection Settings**.

STEP 2 Enter the following global configuration fields:

- **ND Inspection VLAN List**—Enter one or more VLANs on which ND Inspection is enabled.
- **Drop Unsecure**—Select to enable dropping messages with no CGA or RSA Signature option within an IPv6 ND Inspection policy.
- **Minimal Security Level**—If unsecure messages are not dropped, select the security level below which messages are not forwarded.
  - *No Verification*—Disables verification of the security level.
  - *User Defined*—Specify the security level of the message to be forwarded.

STEP 3 If required, click **Add** to create an ND Inspection policy.

STEP 4 Enter the following fields:

- **Policy Name**—Enter a user-defined policy name.
- **Device Role**—Select either **Server** or **Client** to specify the role of the device attached to the port for ND Inspection.
  - *Inherited*—Role of device is inherited from either the VLAN or system default (client).
  - *Client*—Role of device is client.
  - *Host*—Role of device is host.
- **Drop Unsecure**—See above.
- **Minimal Security Level**—See above.
- **Validate Source MAC**—Specify whether to globally enable checking source MAC address against the link-layer address:
  - *Inherited*—Inherit value from VLAN or system default (disabled).
  - *Enable*—Enable checking source MAC address against the link-layer address.
  - *Disable*—Disable checking source MAC address against the link-layer address.

STEP 5 If required, click either **Attach Policy to VLAN** or **Attach Policy to Interface**.

Neighbor Binding Settings

The Neighbor Binding table is a database table of IPv6 neighbors connected to a device is created from information sources, such as Neighbor Discovery Protocol (NDP) snooping. This database, or binding, table is used by various IPv6 guard features to prevent spoofing and redirect attacks.

Use the Neighbor Binding Settings page to enable the Neighbor Binding feature on a specified group of VLANs and to set the global configuration values for this feature. If required, a policy can be added or the system-defined default Neighbor Binding policies can be configured in this page.

To configure Neighbor Binding on ports or LAGs:

STEP 1 Click **Security** > **First Hop Security** > **Neighbor Binding Settings**.

STEP 2 Enter the following global configuration fields:

- **Neighbor Binding VLAN List—**Enter one or more VLANs on which Neighbor Binding is enabled.
- **Manual Neighbor Binding**—Select to indicate that entries can be added to the Neighbor Binding table manually.
- **Neighbor Binding Lifetime—**Enter the length of time that addresses remain in the Neighbor Bindings table.
- **Neighbor Binding Logging—**This field indicates whether to enable validation of a bound IPv6 address against the Neighbor Prefix table and logging of Binding table main events.
- **Neighbor Binding Entry Limits—**Specify the maximum number of Neighbor Binding entries per type of interface or address:
    - *Entries Per VLAN:*—Specifies the neighbor binding limit per number of VLANs.
    - *Entries Per Interface:*—Specifies the neighbor binding limit per interface.
    - *Entries Per MAC Address:*—Specifies the neighbor binding limit per MAC address.

STEP 3 If required, click **Add** to create a Neighbor Binding policy.

STEP 4 Enter the following fields:

- **Policy Name—**Enter a user-defined policy name.
- **Device Role**—Select either **Server** or **Client** to specify the role of the device attached to the port for the Neighbor Binding policy.
  - *Inherited*—Role of device is inherited from either the VLAN or system default (client).
  - *Client*—Role of device is client.
  - *Host*—Role of device is host.
- **Neighbor Binding Logging—**See above.
- **Neighbor Binding Entry Limits—**See above.

STEP 5 If required, click either **Attach Policy to VLAN** or **Attach Policy to Interface**.

Policy Attachment (VLAN)

To attach a policy to one or more VLANs:

STEP 1 Click **Security** > **First Hop Security** > **Policy Attachment (VLAN)**.

The list of policies that are already attached are displayed along with their **Policy Type**, **Policy Name** and **VLAN List**.

STEP 2 To attach a policy to a VLAN, click **Add** and enter the following fields:

- **Policy Type—**Select the policy type to attach to the interface.
- **Policy Name—**Select the name of the policy to attach to the interface
- **VLAN List**—Select the VLANs to which the policy is attached. Select **All VLANs** or enter a range of VLANs.

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

Policy Attachment (Port)

To attach a policy to one or more ports or LAGs:

STEP 1 Click **Security** > **First Hop Security** > **Policy Attachment (Port)**.

The list of policies that are already attached are displayed along with their **Interface** number, **Policy Type**, **Policy Name** and **VLAN List**.

STEP 2 To attach a policy to a port or LAG, click **Add** and enter the following fields:

- **Interface—**Select the interface on which the policy will be attached.
- **Policy Type—**Select the policy type to attach to the interface.
- **Policy Name—**Select the name of the policy to attach to the interface
- **VLAN List—**Select the VLANs to which the policy is attached. Select **All VLANs** or enter a range of VLANs.

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

Neighbor Binding Table

To add or modify entries in the Neighbor Binding table:

STEP 1 Click **Security** > **First Hop Security** > **Neighbor Binding Table**

STEP 2 Select one of the following clear table options:

- **Static Only—**Clear all static entries in the table.
- **Dynamic Only—**Clear all dynamic entries in the table.
- **All Dynamic & Static —**Clear all dynamic and static entries in the table.

STEP 3 Click **Add** to add a new entry to the table.

STEP 4 Enter the following fields:

- **VLAN ID—**VLAN ID of the entry.
- **IPv6 Address—**Source IPv6 address of the entry.
- **Interface Name—** Port on which packet is received.
- **MAC Address—** Neighbor MAC address of the packet.

FHS Status

To display the global configuration for the FHS features:

STEP 1 Click **Security** > **First Hop Security** > **FHS Status.**

STEP 2 Select a port, LAG or VLAN for which the FHS state is reported.

STEP 3 The following fields are displayed for the selected interface:

- **FHS Status**
    - *FHS State on Current VLAN:*—Is FHS enabled on the current VLAN.
    - *Packet Drop Logging:*—Is this feature enabled for the current interface (at the level of global configuration or in a policy attached to the interface).
- **RA Guard Status**
    - *RA Guard State on Current VLAN:*—Is RA Guard enabled on the current VLAN.
    - *Device Role:*—RA device role.
    - *Managed Configuration Flag:*—Is verification of the managed configuration flag enabled.
    - *Other Configuration Flag:*—Is verification of the other configuration flag enabled.
    - *RA Address List:*—RA address list to be matched.
    - *RA Prefix List:*—RA prefix list to be matched.
    - *Minimal Hop Limit:*—Is minimum RA hop limit verification enabled.
    - *Maximal Hop Limit:*—Is maximum RA hop limit verification enabled.
    - *Minimal Router Preference:*—Is minimum router preference verification enabled.
    - *Maximal Router Preference:*—Is maximum router preference verification enabled.
- **ND Inspection Status**
    - *ND Inspection State on Current VLAN:*—Is ND Inspection enabled on the current VLAN.

  - *Device Role:*—ND Inspection device role.
  - *Drop Unsecure:*—Are unsecure messages dropped.
  - *Minimal Security Level:*—If unsecure messages are not dropped, what is the minimum security level for packets to be forwarded.
  - *Validate Source MAC:*—Is source MAC address verification enabled.
- **DHCP Guard Status**
  - *DHCPv6 Guard State on Current VLAN:*—Is DHCPv6 Guard enabled on the current VLAN.
  - *Device Role:*—DHCP device role.
  - *Match Reply Prefixes:*—Is DHCP reply prefixes verification enabled.
  - *Match Server Address:*—Is DHCP server addresses verification enabled.
  - *Minimal Preference:*—Is verification of the minimal preference enabled.
  - *Maximal Preference:*—Is verification of the maximum preference enabled.
- **Neighbor Binding Status**
  - *Neighbor Binding State on Current VLAN:*—Is Neighbor Binding enabled on the current VLAN.
  - *Device Role:*—Neighbor Binding device role.
  - *Logging Binding:*—Is logging of Neighbor Binding table events enabled.
  - *Max Entries per VLAN:*—Maximum number of dynamic Neighbor Binding table entries per VLAN allowed.
  - *Max Entries per Interface:*—Maximum number of Neighbor Binding table entries per interface allowed.
  - *Max Entries per MAC Address:*—Maximum number of Neighbor Binding table entries per MAC address allowed.

FHS Statistics

To display FHS statistics:

STEP 1 Click **Security** > **First Hop Security** > **FHS Statistics:**

STEP 2 The following fields are displayed:

- **NDP (Neighbor Discovery Protocol) Messages**—The number of received and bridged messages are displayed for the following types of messages:
    - *RA*—Router Advertisement messages
    - *CPA*—Certification Path Advertisement messages
    - *ICMPv6*—Internet Control Message IPv6 Protocol messages.
    - *NS*—Neighbor Solicitation messages.
    - *RS*—Router Solicitation message.
    - *CPS*—Certification Path Solicitation messages.
- **DHCPv6 Messages**—The number of received and bridged messages are displayed for the various types of DHCPv6 messages

The following fields are displayed in the FHS Dropped Message Table

- **Protocol**— Dropped message protocol.
- **Message Type**—Type of message dropped.
- **Count**—Number of messages dropped.
- **Reason**—Reason that the messages were dropped.

21

Security: Secure Sensitive Data Management

Secure Sensitive Data (SSD) is an architecture that facilitates the protection of sensitive data on a device, such as passwords and keys. The facility makes use of passphrases, encryption, access control, and user authentication to provide a secure solution to managing sensitive data.

The facility is extended to protect the integrity of configuration files, to secure the configuration process, and to support SSD zero-touch auto configuration.

- **Introduction**
- **SSD Rules**
- **SSD Properties**
- **Configuration Files**
- **SSD Management Channels**
- **Menu CLI and Password Recovery**
- **Configuring SSD**

Introduction

SSD protects sensitive data on a device, such as passwords and keys, permits and denies access to sensitive data encrypted and in plain text based on user credentials and SSD rules, and protects configuration files containing sensitive data from being tampered with.

In addition, SSD enables the secure backup and sharing of configuration files containing sensitive data.

SSD provides users with the flexibility to configure the desired level of protection on their sensitive data; from no protection with sensitive data in plaintext, minimum protection with encryption based on the default passphrase, and better protection with encryption based on user-defined passphrase.

SSD grants read permission to sensitive data only to authenticated and authorized users, and according to SSD rules. A device authenticates and authorizes management access to users through the user authentication process.

Whether or not SSD is used, it is recommended that the administrator secure the authentication process by using the local authentication database, and/or secure the communication to the external authentication servers used in the user authentication process.

In summary, SSD protects sensitive data on a device with SSD rules, SSD properties, and user authentication. And SSD rules, SSD properties, and user authentication configurations of the device are themselves sensitive data protected by SSD.

SSD Management

SSD management includes a collection of configuration parameters that define the handling and security of sensitive data. The SSD configuration parameters themselves are sensitive data and are protected under SSD.

All configuration of SSD is performed through the SSD pages that are only available to users with the correct permissions (see **SSD Rules**).

SSD Rules

SSD rules define the read permissions and default read mode given to a user session on a management channel.

An SSD rule is uniquely identified by its user and SSD management channel. Different SSD rules might exist for the same user but for different channels, and conversely, different rules might exist for the same channel but for different users.

Read permissions determine how sensitive data can be viewed: in only encrypted form, in only plaintext form, in both encrypted or plaintext, or no permission to view sensitive data. The SSD rules themselves are protected as sensitive data.

A device can support a total of 32 SSD rules.

A device grants a user the SSD read permission of the SSD rule that best matches the user identity/credential and the type of management channel from which the user is/will access the sensitive data.

A device comes with a set of default SSD rules. An administrator can add, delete, and change SSD rules as desired.

NOTE A device may not support all the channels defined by SSD.

Elements of an SSD Rule

An SSD rule includes the following elements:

- **User type**—The user types supported in order of most preference to least preference are as follows: (If a user matches multiple SSD rules, the rule with the most preference User Type will be applied).
  - **Specific**—The rule applies to a specific user.
  - **Default User (cisco)**—The rule applies to the default user (cisco).
  - **Level 15**—The rule applies to users with privilege level 15.
  - **All**—The rule applies to all users.
- **User Name**—If user type is Specific, a user name is required.
- **Channel.** Type of SSD management channel to which the rule is applied. The channel types supported are:
  - **Secure**—Specifies the rule applies only to secure channels. Depending on the device, it may support some or all of the following secure channels:
Console port interface, SCP, SSH, and HTTPS.
  - **Insecure**—Specifies that this rule applies only to insecure channels. Depending on the device, it may support some or all of the following insecure channels:
Telnet, TFTP, and HTTP.
  - **Secure XML SNMP**—Specifies that this rule applies only to XML over HTTPS or SNMPv3 with privacy. A device may or may not support all of the secure XML and SNMP channels.
  - **Insecure XML SNMP**—Specifies that this rule applies only to XML over HTTP or SNMPv1/v2 and SNMPv3 without privacy. A device may or may not support all of the secure XML and SNMP channels.
- **Read Permission**—The read permissions associate with the rules. These can be the following:
  - (Lowest) **Exclude**—Users are not permitted to access sensitive data in any form.
  - (Middle) **Encrypted Only**—Users are permitted to access sensitive data as encrypted only.

  - (Higher) **Plaintext Only**—Users are permitted to access sensitive data in plaintext only. Users will also have read and write permission to SSD parameters as well.
  - (Highest) **Both**—Users have both encrypted and plaintext permissions and are permitted to access sensitive data as encrypted and in plaintext. Users will also have read and write permission to SSD parameters as well.

Each management channel allows specific read permissions. The following summarizes these.

Management Channel	Read Permission Options Allowed
Secure	Both, Encrypted Only
Insecure	Both, Encrypted Only
Secure XML SNMP	Exclude, Plaintext Only
Insecure XML SNMP	Exclude, Plaintext Only

- **Default Read Mode**—All default read modes are subjected to the read permission of the rule. The following options exist, but some might be rejected, depending on the read permission. If the user-defined read permission for a user is Exclude (for example), and the default read mode is Encrypted, the user-defined read permission prevails.
  - **Exclude**—Do not allow reading sensitive data.
  - **Encrypted**—Sensitive data is presented in encrypted form.
  - **Plaintext**—Sensitive data is presented in plaintext form.

Each management channel allows specific read presumptions. The following summarizes these.

Read Permission	Default Read Mode Allowed
Exclude	Exclude
Encrypted Only	*Encrypted
Plaintext Only	*Plaintext
Both	*Plaintext, Encrypted

* The Read mode of a session can be temporarily changed in the SSD Properties page if the new read mode does not violate the read permission.

NOTE Note the following:

- The default Read mode for the Secure XML SNMP and Insecure XML SNMP management channels must be identical to their read permission.
- Read permission Exclude is allowed only for Secure XML SNMP and Insecure XML SNMP management channels; Exclude is not allowed for regular secure and insecure channels.
- Exclude sensitive data in secure and Insecure XML-SNMP management channels means that the sensitive data is presented as a 0 (meaning null string or numeric 0). If the user wants to view sensitive data, the rule must be changed to plaintext.
- By default, an SNMPv3 user with privacy and XML-over-secure channels permissions is considered to be a level-15 user.
- SNMP users on Insecure XML and SNMP (SNMPv1,v2, and v3 with no privacy) channel are considered as All users.
- SNMP community names are not used as user names to match SSD rules.
- Access by a specific SNMPv3 user can be controlled by configuring an SSD rule with a user name matching the SNMPv3 user name.
- There must always be at least one rule with read permission: Plaintext Only or Both, because only users with those permissions are able to access the SSD pages.
- Changes in the default read mode and read permissions of a rule will become effective, and will be applied to the affected user(s) and channel of all active management sessions immediately, excluding the session making the changes even if the rule is applicable. When a rule is changed (add, delete, edit), a system will update all the affected CLI/GUI sessions.

  NOTE When the SSD rule applied upon the session login is changed from within that session, the user must log out and back in to see the change.

  NOTE When doing a file transfer initiated by an XML or SNMP command, the underlying protocol used is TFTP. Therefore, the SSD rule for insecure channel will apply.

SSD Rules and User Authentication

SSD grants SSD permission only to authenticated and authorized users and according to the SSD rules. A device depends on its user authentication process to authenticate and authorize management access. To protect a device and its data including sensitive data and SSD configurations from unauthorized access, it is recommended that the user authentication process on a device is secured. To secure the user authentication process, you can use the local authentication database, as well as secure the communication through external authentication servers, such as a RADIUS server. The configuration of the secure communication to the external authentication servers are sensitive data and are protected under SSD.

NOTE The user credential in the local authenticated database is already protected by a non SSD related mechanism

If a user from a channel issues an action that uses an alternate channel, the device applies the read permission and default read mode from the SSD rule that match the user credential and the alternate channel. For example, if a user logs in via a secure channel and starts a TFTP upload session, the SSD read permission of the user on the insecure channel (TFTP) is applied

Default SSD Rules

The device has the following factory default rules:

Table 3

Rule Key		Rule Action	
User	**Channel**	**Read Permission**	**Default Read Mode**
Level 15	Secure XML SNMP	Plaintext Only	Plaintext
Level 15	Secure	Both	Encrypted
Level 15	Insecure	Both	Encrypted
All	Insecure XML SNMP	Exclude	Exclude
All	Secure	Encrypted Only	Encrypted
All	Insecure	Encrypted Only	Encrypted

The default rules can be modified, but they cannot be deleted. If the SSD default rules have been changed, they can be restored.

SSD Default Read Mode Session Override

The system contains sensitive data in a session, as either encrypted or plaintext, based on the read permission and the default read mode of the user.

The default read mode can be temporarily overridden as long it does not conflict with the SSD read permission of the session. This change is effective immediately in the current session, until one of the following occurs:

- User changes it again.
- Session is terminated.
- The read permission of the SSD rule that is applied to the session user is changed and is no longer compatible with the current read mode of the session. In this case, the session read mode returns to the default read mode of the SSD rule.

SSD Properties

SSD properties are a set of parameters that, in conjunction with the SSD rules, define and control the SSD environment of a device. The SSD environment consists of these properties:

- Controlling how the sensitive data is encrypted.
- Controlling the strength of security on configuration files.
- Controlling how the sensitive data is viewed within the current session.

Passphrase

A passphrase is the basis of the security mechanism in the SSD feature, and is used to generate the key for the encryption and decryption of sensitive data. Sx200, Sx300, Sx500, and SG500X/SG500XG/ESW2-550X series switches that have the same passphrase are able to decrypt each other's sensitive data encrypted with the key generated from the passphrase.

A passphrase must comply with the following rules:

- **Length**—Between 8-16 characters.

- **Character Classes**—The passphrase must have at least one upper case character, one lower case character, one numeric character, and one special character e.g. #,$.

Default and User-defined Passphrases

All devices come with a default, out-of-the box passphrase that is transparent to users. The default passphrase is never displayed in the configuration file or in the CLI/GUI.

If better security and protection are desired, an administrator should configure SSD on a device to use a user-defined passphrase instead of the default passphrase. A user-defined passphrase should be treated as a well-guard secret, so that the security of the sensitive data on the device is not compromised.

A user-defined passphrase can be configured manually in plain text. It can also be derived from a configuration file. (See **Sensitive Data Zero-Touch Auto Configuration**). A device always displays user-defined passphrases encrypted.

Local Passphrase

A device maintains a local passphrase which is the passphrase of its Running Configuration. SSD normally performs encryption and decryption of sensitive data with the key generated from the local passphrase.

The local passphrase can be configured to be either the default passphrase or a user-defined passphrase. By default, the local passphrase and default passphrase are identical. It can be changed by administrative actions from either the Command Line Interface (if available) or the web-based interface. It is automatically changed to the passphrase in the startup configuration file, when the startup configuration becomes the running configuration of the device. When a device is reset to factory default, the local passphrase is reset to the default passphrase.

Configuration File Passphrase Control

File passphrase control provides additional protection for a user-defined passphrase, and the sensitive data that are encrypted with the key generated from the user-defined passphrase, in text-based configuration files.

The following are the existing passphrase control modes:

- **Unrestricted** (default)—The device includes its passphrase when creating a configuration file. This enables any device accepting the configuration file to learn the passphrase from the file.
- **Restricted**—The device restricts its passphrase from being exported into a configuration file. Restricted mode protects the encrypted sensitive data in a configuration file from devices that do not have the passphrase. This mode should be used when a user does not want to expose the passphrase in a configuration file.

After a device is reset to the factory default, its local passphrase is reset to the default passphrase. As a result, the device will be not able to decrypt any sensitive data encrypted based on a user-defined passphrase entered from a management session (GUI/CLI), or in any configuration file with restricted mode, including the files created by the device itself before it is reset to factory default. This remains until the device is manually reconfigured with the user-defined passphrase, or learns the user-defined passphrase from a configuration file.

Configuration File Integrity Control

A user can protect a configuration file from being tampered or modified by creating the configuration file with Configuration File Integrity Control. It is recommended that Configuration File Integrity Control be enabled when a device uses a user-defined passphrase with Unrestricted Configuration File Passprhase Control.

CAUTION Any modification made to a configuration file that is integrity protected is considered tampering.

A device determines whether the integrity of a configuration file is protected by examining the File Integrity Control command in the file's SSD Control block. If a file is integrity protected but a device finds the integrity of the file is not intact, the device rejects the file. Otherwise, the file is accepted for further processing.

A device checks for the integrity of a text-based configuration file when the file is downloaded or copied to the Startup Configuration file.

Read Mode

Each session has a Read mode. This determines how sensitive data appears. The Read mode can be either Plaintext, in which case sensitive data appears as regular text, or Encrypted, in which sensitive data appears in its encrypted form.

Configuration Files

A configuration file contains the configuration of a device. A device has a Running Configuration file, a Startup Configuration file, a Mirror Configuration file (optionally), and a Backup Configuration file. A user can manually upload and download a configuration file to and from a remote file-server. A device can automatically download its Startup Configuration from a remote file server during the auto configuration stage using DHCP. Configuration files stored on remote file servers are referred to as remote configuration files.

A Running Configuration file contains the configuration currently being used by a device. The configuration in a Startup Configuration file becomes the Running Configuration after reboot. Running and Startup Configuration files are formatted in internal format. Mirror, Backup, and the remote configuration files are text-based files usually kept for archive, records, or recovery. During copying, uploading, and downloading a source configuration file, a device automatically transforms the source content to the format of the destination file if the two files are of different formats.

File SSD Indicator

When copying the Running or Startup Configuration file into a text-based configuration file, the device generates and places the file SSD indicator in the text-based configuration file to indicate whether the file contains encrypted sensitive data, plaintext sensitive data or excludes sensitive data.

- The SSD indicator, if it exists, must be in the configuration header file.
- A text-based configuration that does not include an SSD indicator is considered not to contain sensitive data.
- The SSD indicator is used to enforce SSD read permissions on text-based configuration files, but is ignored when copying the configuration files to the Running or Startup Configuration file.

The SSD indicator in a file is set according to the user's instruction, during copy, to include encrypted, plaintext or exclude sensitive data from a file.

SSD Control Block

When a device creates a text-based configuration file from its Startup or Running Configuration file, it inserts an SSD control block into the file if a user requests the file is to include sensitive data. The SSD control block, which is protected from tampering, contains SSD rules and SSD properties of the device creating the file. A SSD control block starts and ends with "ssd-control-start" and "ssd-control-end" respectively.

Startup Configuration File

The device currently supports copying from the Running, Backup, Mirror, and Remote Configuration files to a Startup Configuration file. The configurations in the Startup Configuration are effective and become the Running Configuration after reboot. A user can retrieve the sensitive data encrypted or in plaintext from a startup configuration file, subject to the SSD read permission and the current SSD read mode of the management session.

Read access of sensitive data in the startup configuration in any forms is excluded if the passphrase in the Startup Configuration file and the local passphrase are different.

SSD adds the following rules when copying the Backup, Mirror, and Remote Configuration files to the Startup Configuration file:

- After a device is reset to factory default, all of its configurations, including the SSD rules and properties are reset to default.
- If a source configuration file contains encrypted sensitive data, but is missing an SSD control block, the device rejects the source file and the copy fails.
- If there is no SSD control block in the source configuration file, the SSD configuration in the Startup Configuration file is reset to default.
- If there is a passphrase in the SSD control block of the source configuration file, the device will reject the source file, and the copy fails if there is encrypted sensitive data in the file not encrypted by the key generated from the passphrase in the SSD control block.

- If there is an SSD control block in the source configuration file and the file fails the SSD integrity check, and/or file integrity check, the device rejects the source file and fails the copy.
- If there is no passphrase in the SSD control block of the source configuration file, all the encrypted sensitive data in the file must be encrypted by either the key generated from the local passphrase, or the key generated from the default passphrase, but not both. Otherwise, the source file is rejected and the copy fails.
- The device configures the passphrase, passphrase control, and file integrity, if any, from the SSD Control Block in the source configuration file to the Startup Configuration file. It configures the Startup Configuration file with the passphrase that is used to generate the key to decrypt the sensitive data in the source configuration file. Any SSD configurations that are not found are reset to the default.
- If there is an SSD control block in the source configuration file and the file contains plaintext, sensitive data excluding the SSD configurations in the SSD control block, the file is accepted.

Running Configuration File

A Running Configuration file contains the configuration currently being used by the device. A user can retrieve the sensitive data encrypted or in plaintext from a running configuration file, subject to the SSD read permission and the current SSD read mode of the management session. The user can change the Running Configuration by copying the Backup or Mirror Configuration files through other management actions via CLI, XML,SNMP, and so on.

A device applies the following rules when a user directly changes the SSD configuration in the Running Configuration:

- If the user that opened the management session does not have SSD permissions (meaning read permissions of either Both or Plaintext Only), the device rejects all SSD commands.
- When copied from a source file, File SSD indicator, SSD Control Block Integrity, and SSD File Integrity are neither verified nor enforced.
- When copied from a source file, the copy will fail if the passphrase in the source file is in plaintext. If the passphrase is encrypted, it is ignored.
- When directly configuring the passphrase, (non file copy), in the Running Configuration, the passphrase in the command must be entered in plaintext. Otherwise, the command is rejected.

- Configuration commands with encrypted sensitive data, that are encrypted with the key generated from the local passphrase, are configured into the Running Configuration. Otherwise, the configuration command is in error, and is not incorporated into the Running Configuration file.

Backup and Mirror Configuration File

A device periodically generates its Mirror Configuration file from the Startup Configuration file if auto mirror configuration service is enabled. A device always generates a Mirror Configuration file with encrypted sensitive data. Therefore, the File SSD Indicator in a Mirror Configuration file always indicates that the file contains encrypted sensitive data.

By default, auto mirror configuration service is enabled. To configure auto mirror configuration to be enabled or disabled, click **Administration > File Management > Configuration File Properties**.

A user can display, copy, and upload the complete mirror and backup configuration files, subject to SSD read permission, the current read mode in the session, and the file SSD indicator in the source file as follows:

- If there is no file SSD indicator in a mirror or backup configuration file, all users are allowed to access the file.
- A user with Both read permission can access all mirror and backup configuration files. However, if the current read mode of the session is different than the file SSD indicator, the user is presented with a prompt indicating that this action is not allowed.
- A user with Plaintext Only permission can access mirror and backup configuration files if their file SSD Indicator shows Exclude or Plaintext Only sensitive data.
- A user with Encrypted Only permission can access mirror and backup configuration files with their file SSD Indicator showing Exclude or Encrypted sensitive data.
- A user with Exclude permission cannot access mirror and backup configuration files with their file SSD indicator showing either encrypted or plaintext sensitive data.

The user should not manually change the file SSD indicator that conflicts with the sensitive data, if any, in the file. Otherwise, plaintext sensitive data may be unexpectedly exposed.

Sensitive Data Zero-Touch Auto Configuration

SSD Zero-touch Auto Configuration is the auto configuration of target devices with encrypted sensitive data, without the need to manually pre-configure the target devices with the passphrase whose key is used to encrypted the sensitive data.

The device currently supports Auto Configuration, which is enabled by default. When Auto Configuration is enabled on a device and the device receives DHCP options that specify a file server and a boot file, the device downloads the boot file (remote configuration file) into the Startup Configuration file from a file server, and then reboots.

NOTE The file server may be specified by the bootp siaddr and sname fields, as well as DHCP option 150 and statically configured on the device.

The user can safely auto configure target devices with encrypted sensitive data, by first creating the configuration file that is to be used in the auto configuration from a device that contains the configurations. The device must be configured and instructed to:

- Encrypt the sensitive data in the file
- Enforce the integrity of the file content
- Include the secure, authentication configuration commands and SSD rules that properly control and secure the access to devices and the sensitive data

If the configuration file was generated with a user passphrase and SSD file passphrase control is Restricted, the resulting configuration file can be auto-configured to the desired target devices. However, for auto configuration to succeed with a user-defined passphrase, the target devices must be manually pre-configured with the same passphrase as the device that generates the files, which is not zero touch.

If the device creating the configuration file is in Unrestricted passphrase control mode, the device includes the passphrase in the file. As a result, the user can auto configure the target devices, including devices that are out-of-the-box or in factory default, with the configuration file without manually pre-configuring the target devices with the passphrase. This is zero touch because the target devices learn the passphrase directly from the configuration file.

NOTE Devices that are out-of-the-box or in factory default states use the default anonymous user to access the SCP server.

SSD Management Channels

Devices can be managed over management channels such as telnet, SSH, and web. SSD categories the channels into the following types based on their security and/or protocols: secured, insecure, secure-XML-SNMP, and insecure-XML-SNMP.

The following describes whether SSD considers each management channel to be secure or insecure. If it is insecure, the table indicates the parallel secure channel.

Management Channel	SSD Management Channel Type	Parallel Secured Management Channel
Console	Secure	
Telnet	Insecure	SSH
SSH	Secure	
GUI/HTTP	Insecure	GUI/HTTPS
GUI/HTTPS	Secure	
XML/HTTP	Insecure-XML-SNMP	XML/HTTPS
XML/HTTPS	Secure-XML-SNMP	
SNMPv1/v2/v3 without privacy	Insecure-XML-SNMP	Secure-XML-SNMP
SNMPv3 with privacy	Secure-XML-SNMP (level-15 users)	
TFTP	Insecure	SCP
SCP (Secure Copy)	Secure	
HTTP based file transfer	Insecure	HTTPS-based file transfer
HTTPS based file transfer	Secure	

Menu CLI and Password Recovery

The Menu CLI interface is only allowed to users if their read permissions are Both or Plaintext Only. Other users are rejected. Sensitive data in the Menu CLI is always displayed as plaintext.

Password recovery is currently activated from the boot menu and allows the user to log on to the terminal without authentication. If SSD is supported, this option is only permitted if the local passphrase is identical to the default passphrase. If a device is configured with a user-defined passphrase, the user is unable to activate password recovery.

Configuring SSD

The SSD feature is configured in the following pages:

- SSD properties are set in the Properties page.
- SSD rules are defined in the SSD Rules page.

SSD Properties

Only users with SSD read permission of Plaintext-only or Both are allowed to set SSD properties.

To configure global SSD properties:

STEP 1 Click **Security** > **Secure Sensitive Data Management** > **Properties**. The following field appears:

- **Current Local Passphrase Type—**Displays whether the default passphrase or a user-defined passphrase is currently being used.

STEP 2 Enter the following **Persistent Settings** fields:

- **Configuration File Passphrase Control—**Select an option as described in **Configuration File Passphrase Control**.
- **Configuration File Integrity Control—**Select to enable this feature. See **Configuration File Integrity Control**.

STEP 3 Select a Read mode for the current session (see **Elements of an SSD Rule**).

To change the local passphrase:

STEP 1 Click **Change Local Passphrase**, and enter a new **Local Passphrase**:

- **Default—**Use the devices default passphrase.

- **User Defined (Plaintext)**—Enter a new passphrase.
- **Confirm Passphrase**—Confirm the new passphrase.

SSD Rules

Only users with SSD read permission of Plaintext-only or Both are allowed to set SSD rules.

To configure SSD rules:

STEP 1 Click **Security** > **Secure Sensitive Data Management** > **SSD Rules**.

The currently-defined rules are displayed.

STEP 2 To add a new rule, click **Add**. Enter the following fields:

- **User**—This defines the user(s) to which the rule applies: Select one of the following options:
    - *Specific User*—Select and enter the specific user name to which this rule applies (this user does not necessarily have to be defined).
    - *Default User (cisco)*—Indicates that this rule applies to the default user.
    - *Level 15*—Indicates that this rule applies to all users with privilege level 15.
    - *All*—Indicates that this rule applies to all users.
- **Channel**—This defines the security level of the input channel to which the rule applies: Select one of the following options:
    - *Secure*—Indicates that this rule applies only to secure channels (console, SCP, SSH and HTTPS), not including the SNMP and XML channels.
    - *Insecure*—Indicates that this rule applies only to insecure channels (Telnet, TFTP and HTTP), not including the SNMP and XML channels.
    - *Secure XML SNMP*—Indicates that this rule applies only to XML over HTTPS and SNMPv3 with privacy.
    - *Insecure XML SNMP*—Indicates that this rule applies only to XML over HTTP or and SNMPv1/v2and SNMPv3 without privacy.

- **Read Permission—**The read permissions associated with the rule. These can be the following:
    - *Exclude*—Lowest read permission. Users are not permitted to get sensitive data in any form.
    - *Plaintext Only*—Higher read permission than above ones. Users are permitted to get sensitive data in plaintext only.
    - *Encrypted Only*—Middle read permission. Users are permitted to get sensitive data as encrypted only.
    - *Both (Plaintext and Encrypted)*—Highest read permission. Users have both encrypted and plaintext permissions and are permitted to get sensitive data as encrypted and in plaintext
- **Default Read Mode—**All default read modes are subjected to the read permission of the rule. The following options exist, but some might be rejected, depending on the rule's read permission.
    - *Exclude*—Do not allow reading the sensitive data.
    - *Encrypted*—Sensitive data is presented encrypted.
    - *Plaintext*—Sensitive data is presented as plaintext.

STEP 3 The following actions can be performed:

- **Restore to Default—**Restore a user-modified default rule to the default rule.
- **Restore All Rules to Default—**Restore all user-modified default rules to the default rule and remove all user-defined rules.

22

Security: SSH Client

This section describes the device when it functions as an SSH client.

It covers the following topics:

- **Secure Copy (SCP) and SSH**
- **Protection Methods**
- **SSH Server Authentication**
- **SSH Client Authentication**
- **Before You Begin**
- **Common Tasks**
- **SSH Client Configuration Through the GUI**

Secure Copy (SCP) and SSH

Secure Shell or SSH is a network protocol that enables data to be exchanged on a secure channel between an SSH client (in this case, the device) and an SSH server.

SSH client helps the user manage a network composed of one or more switches in which various system files are stored on a central SSH server. When configuration files are transferred over a network, Secure Copy (SCP), which is an application that utilizes the SSH protocol, ensures that sensitive data, such as username/password cannot be intercepted.

Secure Copy (SCP) is used to securely transfer firmware, boot image, configuration files, language files, and log files from a central SCP server to a device.

With respect to SSH, the SCP running on the device is an SSH client application and the SCP server is a SSH server application.

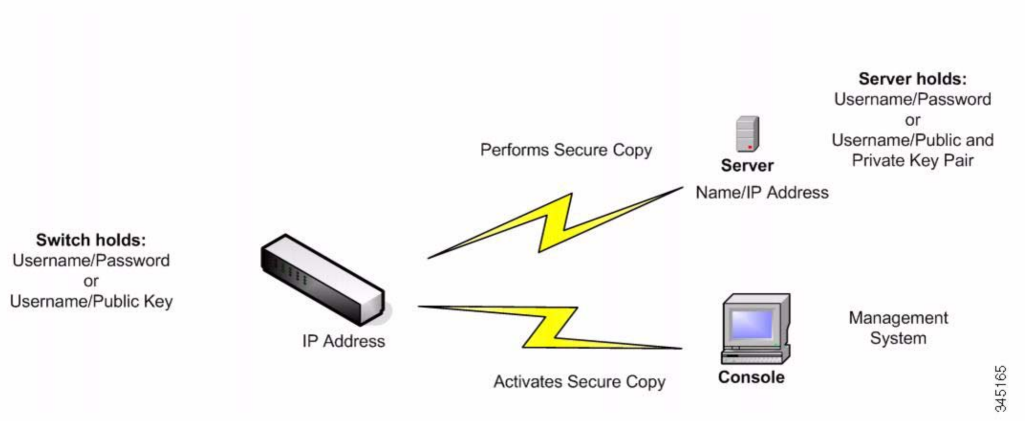
When files are downloaded via TFTP or HTTP, the data transfer is unsecured.

When files are downloaded via SCP, the information is downloaded from the SCP server to the device via a secure channel. The creation of this secure channel is preceded by authentication, which ensures that the user is permitted to perform the operation.

Authentication information must be entered by the user, both on the device and on the SSH server, although this guide does not describe server operations.

The following illustrates a typical network configuration in which the SCP feature might be used.

Typical Network Configuration



Protection Methods

When data is transferred from an SSH server to a device (client), the SSH server uses various methods for client authentication. These are described below.

Passwords

To use the password method, first ensure that a username/password has been established on the SSH server. This is not done through the device's management system, although, after a username has been established on the server, the server password can be changed through the device's management system.

The username/password must then be created on the device. When data is transferred from the server to the device, the username/password supplied by the device must match the username/password on the server.

Data can be encrypted using a one-time symmetric key negotiated during the session.

Each device being managed must have its own username/password, although the same username/password can be used for multiple switches.

The password method is the default method on the device.

Public/Private Keys

To use the public/private key method, create a username and public key on the SSH server. The public key is generated on the device, as described below, and then copied to the server. The actions of creating a username on the server and copying the public key to the server are not described in this guide.

RSA and DSA default key pairs are generated for the device when it is booted. One of these keys is used to encrypt the data being downloaded from the SSH server. The RSA key is used by default.

If the user deletes one or both of these keys, they are regenerated.

The public/private keys are encrypted and stored in the device memory. The keys are part of the device configuration file, and the private key can be displayed to the user, in encrypted or plaintext form.

Since the private key cannot be copied directly to the private key of another device, an import method exists that enables copying private keys from device to device (described in **Import Keys**).

Import Keys

In the key method, individual public/private keys must be created for each individual device, and these private keys cannot be copied directly from one device to another because of security considerations.

If there are multiple switches in the network, the process of creating public/private keys for all the switches might be time-consuming, because each public/private key must be created and then loaded onto the SSH server.

To facilitate this process, an additional feature enables secure transfer of the encrypted private key to all switches in the system.

When a private key is created on a device, it is also possible to create an associated *passphrase*. This passphrase is used to encrypt the private key and to import it into the remaining switches. In this way, all the switches can use the same public/private key.

SSH Server Authentication

A device, as an SSH client, only communicates with a trusted SSH server. When SSH server authentication is disabled (the default setting), any SSH server is considered trusted. When SSH server authentication is enabled, the user must add an entry for the trusted servers to the Trusted SSH Servers Table. This table stores the following information per each SSH Trusted server for a maximum of 16 servers, and contains the following information:

- Server IP address/host name
- Server public key fingerprint

When SSH server authentication is enabled, the SSH client running on the device authenticates the SSH server using the following authentication process:

- The device calculates the fingerprint of the received SSH server's public key.
- The device searches the SSH Trusted Servers table for the SSH server's IP address/host name. One of the following can occur:
    - If a match is found, both for the server's IP address/host name and its fingerprint, the server is authenticated.
    - If a matching IP address/host name is found, but there is no matching fingerprint, the search continues. If no matching fingerprint is found, the search is completed and authentication fails.
    - If no matching IP address/host name is found, the search is completed and authentication fails.
- If the entry for the SSH server is not found in the list of trusted servers, the process fails.

SSH Client Authentication

SSH client authentication by password is enabled by default, with the username/password being “anonymous”.

The user must configure the following information for authentication:

- The authentication method to be used.
- The username/password or public/private key pair.

In order to support auto configuration of an out-of-box device (device with factory default configuration), SSH server authentication is disabled by default.

Supported Algorithms

When the connection between a device (as an SSH client) and an SSH server is established, the client and SSH server exchange data in order to determine the algorithms to use in the SSH transport layer.

The following algorithms are supported on the client side:

- Key Exchange Algorithm-diffie-hellman
- Encryption Algorithms
    - aes128-cbc
    - 3des-cbc
    - arcfour
    - aes192-cbc
    - aes256-cbc
- Message Authentication Code Algorithms
    - hmac-sha1
    - hmac-md5

NOTE Compression algorithms are not supported.

Before You Begin

The following actions must be performed before using the SCP feature:

- When using the password authentication method, a username/password must be set up on the SSH server.
- When using public/private keys authentication method, the public key must be stored on the SSH server.

Common Tasks

This section describes some common tasks performed using the SSH client. All pages referenced are pages found under the SSH Client branch of the menu tree.

Workflow1: To configure SSH client and transfer data to/from an SSH server, perform the following steps:

STEP 1 Decide which method is to be used: password or public/private key. Use the SSH User Authentication page.

STEP 2 If the password method was selected, perform the following steps:

a. Create a global password in the SSH User Authentication page, or create a temporary one in the Upgrade/Backup Firmware/Language or Backup Configuration/Log pages, when you actually activate the secure data transfer.

b. Upgrade the firmware, boot image or language file, using SCP, by selecting the **via SCP (over SSH)** option in the Upgrade/Backup Firmware/Language page. The password can be entered in this page directly, or the password entered in the SSH User Authentication page can be used.

c. Download/backup the configuration file, using SCP, by selecting the **via SCP (over SSH)** option in the Download/Backup Configuration/Log page. The password can be entered in this page directly, or the password entered in the SSH User Authentication page can be used.

STEP 3 Set up a username/password on the SSH server or modify the password on the SSH server. This activity depends on the server and is not described here.

STEP 4 If the public/private key method is being used, perform the following steps:

a. Select whether to use an RSA or DSA key, create a username and then generate the public/private keys.

b. View the generated key by clicking the **Details** button, and transfer the username and public key to the SSH server. This action depends on the server and is not described in this guide.

c. Upgrade/backup the firmware or language file, using SCP, by selecting the **via SCP (over SSH)** option in the Upgrade/Backup Firmware/Language page.

d. Download/backup the configuration file, using SCP, by selecting the **via SCP (over SSH)** option in the Download/Backup Configuration/Log page.

Workflow2: To import the public/private keys from one device to another:

STEP 1 Generate a public/private key in the SSH User Authentication page.

STEP 2 Set the SSD properties and create a new local passphrase in the Secure Sensitive Data Management > Properties page.

STEP 3 Click **Details** to view the generated, encrypted keys, and copy them (including the Begin and End footers) from the Details page to an external device. Copy the public and private keys separately.

STEP 4 Log on to another device and open the SSH User Authentication page. Select the type of key required and click **Edit**. Paste in the public/private keys.

STEP 5 Click **Apply** to copy the public/private keys onto the second device.

Workflow3: To change your password on an SSH server:

STEP 1 Identify the server in the Change User Password on SSH Server page.

STEP 2 Enter the new password.

STEP 3 Click **Apply**.

Workflow4: To define a trusted server:

STEP 1 Enable SSH server authentication in the SSH Server Authentication page.

STEP 2 Click **Add** to add a new server and enter its identifying information.

STEP 3 Click **Apply** to add the server to the Trusted SSH Servers table.

SSH Client Configuration Through the GUI

This section describes the pages used to configure the SSH Client feature.

SSH User Authentication

Use this page to select an SSH user authentication method, set a username and password on the device, if the password method is selected or generate an RSA or DSA key, if the public/private key method is selected.

To select an authentication method, and set the username/password/keys.

STEP 1 Click **Security** > **SSH Client** > **SSH User Authentication.**

STEP 2 Select an **SSH User Authentication Method.** This is the global method defined for the secure copy (SCP). Select one of the options:

- **By Password—**This is the default setting. If this is selected, enter a password or retain the default one.
- **By RSA Public Key—**If this is selected, create an RSA public and Private key in the **SSH User Key Table** block.
- **By DSA Public Key—**If this is selected, create a DSA public/private key in the **SSH User Key Table** block.

STEP 3 Enter the **Username** (no matter what method was selected) or user the default username. This must match the username defined on the SSH server.

STEP 4 If the *By Password* method was selected, enter a password (**Encrypted** or **Plaintext**) or leave the default encrypted password.

STEP 5 Perform one of the following actions:

- **Apply—**The selected authentication methods are associated with the access method.
- **Restore Default Credentials—**The default username and password (anonymous) are restored.
- **Display Sensitive Data As Plaintext—**Sensitive data for the current page appears as plaintext.

The **SSH User Key Table** contains the following fields for each key:

- **Key Type—**RSA or DSA.

- **Key Source—**Auto Generated or User Defined.
- **Fingerprint—**Fingerprint generated from the key.

STEP 6 To handle an RSA or DSA key, select either RSA or DSA and perform one of the following actions:

- **Generate—**Generate a new key.
- **Edit—**Display the keys for copying/pasting to another device.
- **Delete—**Delete the key.
- **Details—**Display the keys.

SSH Server Authentication

To enable SSH server authentication and define the trusted servers:

STEP 1 Click **Security** > **SSH Client** > **SSH Server Authentication.**

STEP 2 Select **Enable** to enable SSH server authentication.

- **IPv4 Source Interface—**Select the source interface whose IPv4 address will be used as the source IPv4 address for messages used in communication with IPv4 SSH servers.
- **IPv6 Source Interface—**Select the source interface whose IPv6 address will be used as the source IPv6 address for messages used in communication with IPv6 SSH servers.

  NOTE If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

STEP 3 Click **Add** and enter the following fields for the SSH trusted server:

- **Server Definition—**Select one of the following ways to identify the SSH server:
  - *By IP Address*—If this is selected enter the IP address of the server in the fields below.
  - *By Name*—If this is selected enter the name of the server in the **Server IP Address/Name** field.

- **IP Version**—If you selected to specify the SSH server by IP address, select whether that IP address is an IPv4 or IPv6 address.
- **IP Address Type**—If the SSH server IP address is an IPv6 address, select the IPv6 address type. 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 from the list of interfaces.
- **Server IP Address/Name**—Enter either the IP address of the SSH server or its name, depending on what was selected in **Server Definition**.
- **Fingerprint**—Enter the fingerprint of the SSH server (copied from that server).

STEP 4 Click **Apply**. The trusted server definition is stored in the Running Configuration file.

Changing the User Password on the SSH Server

To change the password on the SSH server:

STEP 1 Click **Security** > **SSH Client** > **Change User Password on SSH Server.**

STEP 2 Enter the following fields:

- **Server Definition**—Define the SSH server by selecting either **By IP Address** or **By Name**. Enter the server name or IP address of the server in the **Server IP Address/Name** field.
- **IP Version**—If you selected to specify the SSH server by IP address, select whether that IP address is an IPv4 or IPv6 address.
- **IP Address Type**—If the SSH server IP address is an IPv6 address, select the IPv6 address type. 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 from the list of interfaces.
- **Server IP Address/Name**—Enter either the IP address of the SSH server or its name, depending on what was selected in **Server Definition**.
- **Username—**This must match the username on the server.
- **Old Password—**This must match the password on the server.
- **New Password—**Enter the new password and confirm it in the **Confirm Password** field.

STEP 3 Click **Apply**. The password on the SSH server is modified.

23

Security: SSH Server

This section describes how to establish an SSH session on the device.

It covers the following topics:

- **Overview**
- **Common Tasks**
- **SSH Server Configuration Pages**

Overview

The SSH Server feature enables users to create an SSH session to the device. This is similar to establishing a telnet session, except that the session is secured.

Public and private keys are automatically generated on the device. These can be modified by the user.

The SSH session is opened using a special SSH client application, such as PuTTY.

SSH Server can operate in the following modes:

- **By Internally-generated RSA/DSA Keys (Default Setting)**—An RSA and a DSA key are generated. Users log on the SSH Server application and are automatically authenticated to open a session on the device when they supply the IP address of the device.
- **Public Key Mode**—Users are defined on the device. Their RSA/DSA keys are generated in an external SSH server application, such as PuTTY. The public keys are entered in the device. The users can then open an SSH session on the device through the external SSH server application.

Common Tasks

This section describes some common tasks performed using the SSH Server feature.

Workflow1: To logon to the device over SSH using the device's automatically-created (default) key, perform the following:

STEP 1 Enable SSH server in the TCP/UDP Services page and verify that SSH user authentication by public key is disabled in the SSH User Authentication page.

STEP 2 Log onto an external SSH client application, such as PuTTY, using the IP address of the device (it is not necessary to use a username or key that is known to the device).

Workflow2: To create an SSH user and logon to the device over SSH using this user, perform the following steps:

STEP 1 Generate an RSA or DSA key on an external SSH client application, such as PuTTY.

STEP 2 Enable SSH user authentication by public key or password in the SSH User Authentication page.

STEP 3 Enable Automatic Login if required (see **Automatic Login** below).

STEP 4 Add a user in the SSH User Authentication page and copy in the public key generated externally.

STEP 5 Log onto an external SSH client application, such as PuTTY, using the IP address of the device and the user name of the user.

Workflow3: To import an RSA or DSA key from device A to device B, perform the following steps:

STEP 1 On device A, select an RSA or DSA key in the SSH Server Authentication page.

STEP 2 Click **Details** and copy the public key of the select key type to Notepad or other text editor application.

STEP 3 Log on to device B and open the SSH Server Authentication page. Select either the RSA or DSA key, click **Edit** and paste in the key from device A.

SSH Server Configuration Pages

This section describes the pages used to configure the **SSH Server** feature.

SSH User Authentication

Use the SSH User Authentication page to enable SSH user authentication by public key and/or password, and (when using authentication by public key) to add an SSH client user that will be used to create an SSH session in an external SSH application (like PuTTY).

Before you can add a user, you must generate an RSA or DSA key for the user in the external SSH key generation/client application (such as PuTTY).

Automatic Login

If you use the SSH User Authentication page to create an SSH username for a user who is already configured in the local user database. You can prevent additional authentication by configuring the **Automatic Login** feature, which works as follows:

- **Enabled**—If a user is defined in the local database, and this user passed SSH Authentication using a public-key, the authentication by the local database username and password is skipped.

  NOTE The configured authentication method for this specific management method (console, Telnet, SSH and so on) must be *Local* (i.e. not *RADIUS* or *TACACS+*). See **Management Access Method** for more details).

- **Not Enabled**—After successful authentication by SSH public key, even if the username is configured in the local user database, the user is authenticated again, as per the configured authentication methods, configured on the Management Access Authentication page.

This page is optional. You do not have to work with user authentication in SSH.

To enable authentication and add a user.

STEP 1 Click **Security** > **SSH Server** > SSH User Authentication.

STEP 2 Select the following fields:

- **SSH User Authentication by Password**—Select to perform authentication of the SSH client user using the username/password configured in the local database (see **Defining Users**).

- **SSH User Authentication by Public Key—**Select to perform authentication of the SSH client user using the public key.
- **Automatic Login—**This field can be enabled if the **SSH User Authentication by Public Key** feature was selected. See **Automatic Login**.

The following fields are displayed for the configured users:

- **SSH User Name—**User name of user.
- **Key Type—**Whether this is an RSA or DSA key.
- **Fingerprint—**Fingerprint generated from the public keys.

STEP 3 Click **Add** to add a new user and enter the fields:

- **SSH User Name—**Enter a user name.
- **Key Type—**Select either **RSA** or **DSA**.
- **Public Key—**Copy the public key generated by an external SSH client application (like PuTTY) into this text box.

SSH Server Authentication

A public and private RSA and DSA key are automatically generated when the device is booted from factory defaults. Each key is also automatically created when the appropriate user-configured key is deleted by the user.

To regenerate an RSA or DSA key or to copy in an RSA/DSA key generated on another device:

STEP 1 Click **Security** > **SSH Server** > **SSH Server Authentication**.

The following fields are displayed for each key:

- **Key Type—**RSA or DSA.
- **Key Source—**Auto Generated or User Defined.
- **Fingerprint—**Fingerprint generated from the key.

STEP 2 Select either an RSA or DSA key.

STEP 3 You can perform any of the following actions:

- **Generate—**Generates a key of the selected type.

- **Edit**—Enables you to copy in a key from another device.
- **Delete**—Enables you to delete a key.
- **Details**—Enables you to view the generated key. The Details window also enables you to click **Display Sensitive Data as Plaintext**. If this is clicked, the keys are displayed as plaintext and not in encrypted form. If the key is already being displayed as plaintext, you can click **Display Sensitive Data as Encrypted**. to display the text in encrypted form.

STEP 4 If new keys were copied in from another, click **Apply**. The key(s) are stored in the Running Configuration file.

24

Access Control

The Access Control List (ACL) feature is part of the security mechanism. ACL definitions serve as one of the mechanisms to define traffic flows that are given a specific Quality of Service (QoS). For more information see **Quality of Service**.

ACLs enable network managers to define patterns (filter and actions) for ingress traffic. Packets, entering the device on a port or LAG with an active ACL, are either admitted or denied entry.

This section contains the following topics:

- **Access Control Lists**
- **Defining MAC-based ACLs**
- **IPv4-based ACLs**
- **IPv6-Based ACLs**
- **Defining ACL Binding**

Access Control Lists

An Access Control List (ACL) is an ordered list of classification filters and actions. Each single classification rule, together with its action, is called an Access Control Element (ACE).

Each ACE is made up of filters that distinguish traffic groups and associated actions. A single ACL may contain one or more ACEs, which are matched against the contents of incoming frames. Either a DENY or PERMIT action is applied to frames whose contents match the filter.

The device supports a maximum of 512 ACLs, and a maximum of 512 ACEs.

When a packet matches an ACE filter, the ACE action is taken and that ACL processing is stopped. If the packet does not match the ACE filter, the next ACE is processed. If all ACEs of an ACL have been processed without finding a match, and if another ACL exists, it is processed in a similar manner.

NOTE If no match is found to any ACE in all relevant ACLs, the packet is dropped (as a default action). Because of this default drop action you must explicitly add ACEs into the ACL to permit the desired traffic, including management traffic, such as Telnet, HTTP or SNMP that is directed to the device itself. For example, if you do not want to discard all the packets that do not match the conditions in an ACL, you must explicitly add a lowest priority ACE into the ACL that permits all the traffic.

If IGMP/MLD snooping is enabled on a port bound with an ACL, add ACE filters in the ACL to forward IGMP/MLD packets to the device. Otherwise, IGMP/MLD snooping fails at the port.

The order of the ACEs within the ACL is significant, since they are applied in a first-fit manner. The ACEs are processed sequentially, starting with the first ACE.

ACLs can be used for security, for example by permitting or denying certain traffic flows, and also for traffic classification and prioritization in the QoS Advanced mode.

NOTE A port can be either secured with ACLs or configured with advanced QoS policy, but not both.

There can only be one ACL per port, with the exception that it is possible to associate both an IP-based ACL and an IPv6-based ACL with a single port.

To associate more than one ACL with a port, a policy with one or more class maps must be used.

The following types of ACLs can be defined (depending on which part of the frame header is examined):

- MAC ACL—Examines Layer 2 fields only, as described in *Defining MAC-based ACLs*
- IP ACL—Examines the Layer 3 layer of IP frames, as described in *IPv4-based ACLs*
- IPv6 ACL—Examines the Layer 3 layer of IPv4 frames as described in *Defining IPv6-Based ACL*

If a frame matches the filter in an ACL, it is defined as a flow with the name of that ACL. In advanced QoS, these frames can be referred to using this Flow name, and QoS can be applied to these frames (see **QoS Advanced Mode**).

Creating ACLs Workflow

To create ACLs and associate them with an interface, perform the following:

1. Create one or more of the following types of ACLs:
    a. MAC-based ACL by using the MAC Based ACL page and the MAC Based ACE page
    b. IP-based ACL by using the IPv4 Based ACL page and the IPv4 Based ACE page
    c. IPv6-based ACL by using the IPv6 Based ACL page and the IPv6 Based ACE page
2. Associate the ACL with interfaces by using the ACL Binding page.

Modifying ACLs Workflow

An ACL can only be modified if it is not in use. The following describes the process of unbinding an ACL in order to modify it:

1. If the ACL does not belong to a QoS Advanced Mode class map, but it has been associated with an interface, unbind it from the interface using the ACL Binding page.
2. If the ACL is part of the class map and not bound to an interface, then it can be modified.
3. If the ACL is part of a class map contained in a policy bound to an interface, you must perform the chain of unbinding as follows:
    - Unbind the policy containing the class map from the interface by using *Policy Binding.*
    - Delete the class map containing the ACL from the policy using the *Configuring a Policy* (**Edit**).
    - Delete the class map containing the ACL, by using *Defining Class Mapping*.

Only then can the ACL be modified, as described in this section.

Defining MAC-based ACLs

MAC-based ACLs are used to filter traffic based on Layer 2 fields. MAC-based ACLs check all frames for a match.

MAC-based ACLs are defined in the MAC Based ACL page. The rules are defined in the MAC Based ACE page.

To define a MAC-based ACL:

STEP 1 Click **Access Control** > **MAC-Based ACL**.

This page contains a list of all currently-defined MAC-based ACLs.

STEP 2 Click **Add**.

STEP 3 Enter the name of the new ACL in the **ACL Name** field. ACL names are case-sensitive.

STEP 4 Click **Apply**. The MAC-based ACL is saved to the Running Configuration file.

Adding Rules to a MAC-based ACL

NOTE Each MAC-based rule consumes one TCAM rule. Note that the TCAM allocation is performed in couples, such that, for the first ACE, 2 TCAM rules are allocated and the second TCAM rule is allocated to the next ACE, and so forth.

To add rules (ACEs) to an ACL:

STEP 1 Click **Access Control** > **Mac-Based ACE**.

STEP 2 Select an ACL, and click **Go**. The ACEs in the ACL are listed.

STEP 3 Click **Add**.

STEP 4 Enter the parameters.

- **ACL Name—**Displays the name of the ACL to which an ACE is being added.
- **Priority—**Enter the priority of the ACE. ACEs with higher priority are processed first. One is the highest priority.
- **Action—**Select the action taken upon a match. The options are:
    - *Permit*—Forward packets that meet the ACE criteria.
    - *Deny*—Drop packets that meet the ACE criteria.
    - *Shutdown*—Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.

- **Time Range**—Select to enable limiting the use of the ACL to a specific time range.
- **Time Range Name**—If **Time Range** is selected, select the time range to be used. Time ranges are defined in the **<300-500>Time Range** section.
- **Destination MAC Address**—Select *Any* if all destination addresses are acceptable or *User defined* to enter a destination address or a range of destination addresses.
- **Destination MAC Address Value**—Enter the MAC address to which the destination MAC address is to be matched and its mask (if relevant).
- **Destination MAC Wildcard Mask**—Enter the mask to define a range of MAC addresses. Note that this mask is different than in other uses, such as subnet mask. Here, setting a bit as **1** indicates don't care and **0** indicates to mask that value.

  NOTE Given a mask of 0000 0000 0000 0000 0000 0000 1111 1111 (which means that you match on the bits where there is 0 and don't match on the bits where there are 1's). You need to translate the 1's to a decimal integer and you write 0 for each four zeros. In this example since 1111 1111 = 255, the mask would be written: as 0.0.0.255.
- **Source MAC Address**—Select *Any* if all source address are acceptable or *User defined* to enter a source address or range of source addresses.
- **Source MAC Address Value**—Enter the MAC address to which the source MAC address is to be matched and its mask (if relevant).
- **Source MAC Wildcard Mask**—Enter the mask to define a range of MAC addresses.
- **VLAN ID**—Enter the VLAN ID section of the VLAN tag to match.
- **802.1p**—Select **Include** to use 802.1p.
- **802.1p Value**—Enter the 802.1p value to be added to the VPT tag.
- **802.1p Mask**—Enter the wildcard mask to be applied to the VPT tag.
- **Ethertype**—Enter the frame Ethertype to be matched.

STEP 5 Click **Apply**. The MAC-based ACE is saved to the Running Configuration file.

IPv4-based ACLs

IPv4-based ACLs are used to check IPv4 packets, while other types of frames, such as ARPs, are not checked.

The following fields can be matched:

- IP protocol (by name for well-known protocols, or directly by value)
- Source/destination ports for TCP/UDP traffic
- Flag values for TCP frames
- ICMP and IGMP type and code
- Source/destination IP addresses (including wildcards)
- DSCP/IP-precedence value

NOTE ACLs are also used as the building elements of flow definitions for per-flow QoS handling (see **QoS Advanced Mode**).

The IPv4 Based ACL page enables adding ACLs to the system. The rules are defined in the IPv4 Based ACE page.

IPv6 ACLs are defined in the IPv6 Based ACL page.

Defining an IPv4-based ACL

To define an IPv4-based ACL:

STEP 1 Click **Access Control** > **IPv4-Based ACL**.

This page contains all currently defined IPv4-based ACLs.

STEP 2 Click **Add**.

STEP 3 Enter the name of the new ACL in the **ACL Name** field. The names are case-sensitive.

STEP 4 Click **Apply**. The IPv4-based ACL is saved to the Running Configuration file.

Adding Rules (ACEs) to an IPv4-Based ACL

NOTE Each IPv4-based rule consumes one TCAM rule. Note that the TCAM allocation is performed in couples, such that, for the first ACE, 2 TCAM rules are allocated and the second TCAM rule is allocated to the next ACE, and so forth.

To add rules (ACEs) to an IPv4-based ACL:

STEP 1 Click **Access Control** > **IPv4-Based ACE**.

STEP 2 Select an ACL, and click **Go**. All currently-defined IP ACEs for the selected ACL are displayed.

STEP 3 Click **Add**.

STEP 4 Enter the parameters.

- **ACL Name—**Displays the name of the ACL.
- **Priority—**Enter the priority. ACEs with higher priority are processed first.
- **Action—**Select the action assigned to the packet matching the ACE. The options are as follows:
    - *Permit*—Forward packets that meet the ACE criteria.
    - *Deny*—Drop packets that meet the ACE criteria.
    - *Shutdown*—Drop packet that meets the ACE criteria and disable the port to which the packet was addressed. Ports are reactivated from the Port Management page.
- **Time Range—**Select to enable limiting the use of the ACL to a specific time range.
- **Time Range Name—**If **Time Range** is selected, select the time range to be used. Time ranges are defined in the **<300-500>Time Range** section.
- **Protocol—**Select to create an ACE based on a specific protocol or protocol ID. Select *Any (IPv4)* to accept all IP protocols. Otherwise select one of the following protocols from the drop-down list:
    - *ICMP*—Internet Control Message Protocol
    - *IGMP*—Internet Group Management Protocol
    - *IP in IP*—IP in IP encapsulation
    - *TCP*—Transmission Control Protocol

  - *EGP*—Exterior Gateway Protocol
  - *IGP*—Interior Gateway Protocol
  - *UDP*—User Datagram Protocol
  - *HMP*—Host Mapping Protocol
  - *RDP*—Reliable Datagram Protocol.
  - *IDPR*—Inter-Domain Policy Routing Protocol
  - *IPV6*—IPv6 over IPv4 tunneling
  - *IPV6:ROUT*—Matches packets belonging to the IPv6 over IPv4 route through a gateway
  - *IPV6:FRAG*—Matches packets belonging to the IPv6 over IPv4 Fragment Header
  - *IDRP*—Inter-Domain Routing Protocol
  - *RSVP*—ReSerVation Protocol
  - *AH*—Authentication Header
  - *IPV6:ICMP*—Internet Control Message Protocol
  - *EIGRP*—Enhanced Interior Gateway Routing Protocol
  - *OSPF*—Open Shortest Path First
  - *IPIP*—IP in IP
  - *PIM*—Protocol Independent Multicast
  - *L2TP*—Layer 2 Tunneling Protocol
  - *ISIS*—IGP-specific protocol
- **Protocol ID to Match**—Instead of selecting the name, enter the protocol ID.
- **Source IP Address**—Select *Any* if all source address are acceptable or *User defined* to enter a source address or range of source addresses.
- **Source IP Address Value**—Enter the IP address to which the source IP address is to be matched.

- **Source IP Wildcard Mask—**Enter the mask to define a range of IP addresses. Note that this mask is different than in other uses, such as subnet mask. Here, setting a bit as 1 indicates don't care and 0 indicates to mask that value.

  NOTE Given a mask of 0000 0000 0000 0000 0000 0000 1111 1111 (which means that you match on the bits where there is 0 and don't match on the bits where there are 1's). You need to translate the 1's to a decimal integer and you write 0 for each four zeros. In this example since 1111 1111 = 255, the mask would be written: as 0.0.0.255.

- **Destination IP Address—**Select *Any* if all destination address are acceptable or *User defined* to enter a destination address or range of destination addresses.
- **Destination IP Address Value—**Enter the IP address to which the destination IP address is to be matched.
- **Destination IP Wildcard Mask—**Enter the mask to define a range of IP addresses.
- **Source Port—**Select one of the following:
  - *Any*—Match to all source ports.
  - *Single*—Enter a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is selected in the Select from List drop-down menu.
  - *Range*—Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
- **Destination Port—**Select one of the available values that are the same as the Source Port field described above.

  NOTE You must specify the IP protocol for the ACE before you can enter the source and/or destination port.

- **TCP Flags—**Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security.
- **Type of Service—The service type of the IP packet.**
  - *Any*—Any service type

  - *DSCP to Match*—Differentiated Serves Code Point (DSCP) to match
  - *IP Precedence to match*—IP precedence is a model of TOS (type of service) that the network uses to help provide the appropriate QoS commitments. This model uses the 3 most significant bits of the service type byte in the IP header, as described in RFC 791 and RFC 1349.
- **ICMP**—If the IP protocol of the ACL is ICMP, select the ICMP message type used for filtering purposes. Either select the message type by name or enter the message type number:
  - *Any*—All message types are accepted.
  - *Select from list*—Select message type by name.
  - *ICMP Type to Match*—Number of message type to be used for filtering purposes.
- **ICMP Code**—The ICMP messages can have a code field that indicates how to handle the message. Select one of the following options to configure whether to filter on this code:
  - *Any*—Accept all codes.
  - *User Defined*—Enter an ICMP code for filtering purposes.
- **IGMP**—If the ACL is based on IGMP, select the IGMP message type to be used for filtering purposes. Either select the message type by name or enter the message type number:
  - *Any*—All message types are accepted.
  - *Select from list*—Select message type by name.
  - *IGMP Type to match*—Number of message type that is to be used for filtering purposes.

STEP 5 Click **Apply**. The IPv4-based ACE is saved to the Running Configuration file.

IPv6-Based ACLs

The IPv6-Based ACL page displays and enables the creation of IPv6 ACLs, which check pure IPv6-based traffic. IPv6 ACLs do not check IPv6-over-IPv4 or ARP packets.

NOTE ACLs are also used as the building elements of flow definitions for per-flow QoS handling (see **QoS Advanced Mode**).

Defining an IPv6-based ACL

To define an IPv6-based ACL:

STEP 1 Click **Access Control** > **IPv6-Based ACL**.

This window contains the list of defined ACLs and their contents

STEP 2 Click **Add**.

STEP 3 Enter the name of a new ACL in the **ACL Name** field. The names are case-sensitive.

STEP 4 Click **Apply**. The IPv6-based ACL is saved to the Running Configuration file.

Adding Rules (ACEs) for an IPv6-Based ACL

NOTE Each IPv6-based rule consumes two TCAM rules.

STEP 1 Click **Access Control** > **IPv6-Based ACE**.

This window contains the ACE (rules) for a specified ACL (group of rules).

STEP 2 Select an ACL, and click **Go**. All currently-defined IP ACEs for the selected ACL are displayed.

STEP 3 Click **Add**.

STEP 4 Enter the parameters.

- **ACL Name**—Displays the name of the ACL to which an ACE is being added.
- **Priority**—Enter the priority. ACEs with higher priority are processed first.
- **Action**—Select the action assigned to the packet matching the ACE. The options are as follows:
  - *Permit*—Forward packets that meet the ACE criteria.
  - *Deny*—Drop packets that meet the ACE criteria.
  - *Shutdown*—Drop packets that meet the ACE criteria, and disable the port to which the packets were addressed. Ports are reactivated from the Port Management page.

- **Time Range**—Select to enable limiting the use of the ACL to a specific time range.
- **Time Range Name**—If Time Range is selected, select the time range to be used. Time ranges are described in the **<300-500>Time Range** section.
- **Protocol**—Select to create an ACE based on a specific protocol. Select *Any (IPv6)* to accept all IP protocols. Otherwise select one of the following protocols:
  - *TCP*—Transmission Control Protocol. Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees that packets are transmitted and received in the order they were sent.
  - *UDP*—User Datagram Protocol. Transmits packets but does not guarantee their delivery.
  - *ICMP*—Matches packets to the Internet Control Message Protocol (ICMP).
- **Protocol ID to Match**—Enter the ID of the protocol to be matched.
- **Source IP Address**—Select *Any* if all source address are acceptable or *User defined* to enter a source address or range of source addresses.
- **Source IP Address Value**—Enter the IP address to which the source IP address is to be matched and its mask (if relevant).
- **Source IP Prefix Length**—Enter the prefix length of the source IP address.
- **Destination IP Address**—Select *Any* if all destination address are acceptable or *User defined* to enter a destination address or a range of destination addresses.
- **Destination IP Address Value**—Enter the IP address to which the destination MAC address is matched and its mask (if relevant).
- **Destination IP Prefix Length**—Enter the prefix length of the IP address.
- **Source Port**—Select one of the following:
  - *Any*—Match to all source ports.
  - *Single*—Enter a single TCP/UDP source port to which packets are matched. This field is active only if 800/6-TCP or 800/17-UDP is selected in the IP Protocol drop-down menu.

  - *Range*—Select a range of TCP/UDP source ports to which the packet is matched.

- **Destination Port**—Select one of the available values. (They are the same as for the Source Port field described above).

  NOTE You must specify the IPv6 protocol for the ACL before you can configure the source and/or destination port.

- **TCP Flags**—Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security.
  - Set—Match if the flag is SET.
  - Unset—Match if the flag is Not SET.
  - Dont care—Ignore the TCP flag.
- **Type of Service**—The service type of the IP packet.
- **ICMP**—If the ACL is based on ICMP, select the ICMP message type that is used for filtering purposes. Either select the message type by name or enter the message type number. If all message types are accepted, select *Any*.
  - *Any*—All message types are accepted.
  - *Select from list*—Select message type by name from the drop-down list.
  - *ICMP Type to Match*—Number of message type that is to be used for filtering purposes.
- **ICMP Code**—The ICMP messages may have a code field that indicates how to handle the message. Select one of the following options, to configure whether to filter on this code:
  - *Any*—Accept all codes.
  - *User Defined*—Enter an ICMP code for filtering purposes.

STEP 5 Click **Apply**.

Defining ACL Binding

When an ACL is bound to an interface (port, LAG or VLAN), its ACE rules are applied to packets arriving at that interface. Packets that do not match any of the ACEs in the ACL are matched to a default rule, whose action is to drop unmatched packets.

Although each interface can be bound to only one ACL, multiple interfaces can be bound to the same ACL by grouping them into a policy-map, and binding that policy-map to the interface.

After an ACL is bound to an interface, it cannot be edited, modified, or deleted until it is removed from all the ports to which it is bound or in use.

NOTE It is possible to bind an interface (port, LAG or VLAN) to a policy or to an ACL, but they cannot be bound to both a policy and an ACL.

To bind an ACL to a port or LAG:

STEP 1 Click **Access Control** > **ACL Binding (Port)**.

STEP 2 Select an interface type **Ports/LAGs** (Port or LAG).

STEP 3 Click **Go**. For each type of interface selected, all interfaces of that type are displayed with a list of their current ACLs:

- **Interface**—Identifier of interface.
- **MAC ACL**—ACLs of type MAC that are bound to the interface (if any).
- **IPv4 ACL**—ACLs of type IPv4 that are bound to the interface (if any).
- **IPv6 ACL**—ACLs of type IPv6 that are bound to the interface (if any).

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

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

STEP 5 Select one of the following:

- **Select MAC Based ACL**—Select a MAC-based ACL to be bound to the interface.
- **Select IPv4 Based ACL**—Select an IPv4-based ACL to be bound to the interface.
- **Select IPv6 Based ACL**—Select an IPv6-based ACL to be bound to the interface.

- **Default Action**—Select one of the following options:
  - *Deny Any*—If packet does not match an ACL, it is denied (dropped).
  - *Permit Any*—If packet does not match an ACL, it is permitted (forwarded).

  NOTE Default Action can be defined only if IP Source Guard is not activated on the interface.

STEP 6 Click **Apply**. The ACL binding is modified, and the Running Configuration file is updated.

NOTE If no ACL is selected, the ACL(s) that is previously bound to the interface are unbound.

To bind an ACL to a VLAN:

STEP 1 Click **Access Control** > **ACL Binding (VLAN)**.

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

If the VLAN you require is not displayed, add a new one.

STEP 3 Select one of the following:

- **Select MAC Based ACL**—Select a MAC-based ACL to be bound to the interface.
- **Select IPv4 Based ACL**—Select an IPv4-based ACL to be bound to the interface.
- **Select IPv6 Based ACL**—Select an IPv6-based ACL to be bound to the interface.
- **Default Action**—Select one of the following options:
  - *Deny Any*—If packet does not match an ACL, it is denied (dropped).
  - *Permit Any*—If packet does not match an ACL, it is permitted (forwarded).

  NOTE Default Action can be defined only if IP Source Guard is not activated on the interface.

STEP 4 Click **Apply**. The ACL binding is modified, and the Running Configuration file is updated.

NOTE If no ACL is selected, the ACL(s) that is previously bound to the VLAN are unbound.

25

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 covers the following topics:

- **QoS Features and Components**
- **Configuring QoS - General**
- **QoS Basic Mode**
- **QoS Advanced Mode**
- **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. See **Configuring QoS Queues**.
- **Other Traffic Class-Handling Attribute**—Applies QoS mechanisms to various classes, including bandwidth management.

QoS Operation

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 Modes

The QoS mode that is selected applies to all interfaces in the system.

- **Basic Mod**e—Class of Service (CoS).

  All traffic of the same class receives the same treatment, which is the single QoS action of determining the egress queue on the egress port, based on the indicated QoS value in the incoming frame. This can be 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 device trusts this external assigned QoS value. The external assigned QoS value of a packet determines its traffic class and QoS.

  The header field to be trusted is entered in the Global Settings page. For every value of that field, an egress queue is assigned where 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).

- **Advanced Mode—**Per-flow Quality of Service (QoS).

  In advanced mode, a per flow QoS consists of a class map and/or a policer:

  - A class map defines the kind of traffic in a flow, and contains one or more ACLs. Packets that match the ACLs belong to the flow.
  - A policer applies the configured QoS to a flow. The QoS configuration of a flow may consist of egress queue, the DSCP or CoS/802.1p value, and actions on out of profile (excess) traffic.

- **Disable Mode—**In this mode all traffic is mapped to a single best effort queue, so that no type of traffic is prioritized over another.

Only a single mode can be active at a time. When the system is configured to work in QoS Advanced mode, settings for QoS Basic mode are not active and vice versa.

When the mode is changed, the following occurs:

- When changing from QoS Advanced mode to any other mode, policy profile definitions and class maps are deleted. ACLs bonded directly to interfaces remain bonded.
- When changing from QoS Basic mode to Advanced mode, the QoS Trust mode configuration in Basic mode is not retained.

- When disabling QoS, the shaper and queue setting (WRR/SP bandwidth setting) are reset to default values.

All other user configurations remain intact.

QoS Workflow

To configure general QoS parameters, perform the following:

STEP 1 Choose the QoS mode (Basic, Advanced, or Disabled, as described in the **"QoS Modes"** section) for the system by using the QoS Properties page. The following steps in the workflow, assume that you have chosen to enable QoS.

STEP 2 Assign each interface a default CoS 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 device 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 device is in CoS/802.1 trusted mode, all incoming packets are 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 If required for Layer 3 traffic only, assign a queue to each DSCP/TC value, by using the DSCP to Queue page.

STEP 7 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.

STEP 8 Configure the selected mode by performing one of the following:

a. Configure Basic mode, as described in *Workflow to Configure Basic QoS Mode*

b. Configure Advanced mode, as described in *Workflow to Configure Advanced QoS Mode*.

Configuring QoS - General

The QoS Properties Page contains fields for setting the QoS mode for the system (Basic, Advanced, or Disabled, as described in the **"QoS Modes"** section). In addition, the default CoS priority for each interface can be defined.

Setting QoS Properties

To select the QoS mode:

STEP 1 Click **Quality of Service** > **General** > **QoS Properties**.

STEP 2 Set the QoS mode. The following options are available:

- **Disable**—QoS is disabled on the device.
- **Basic**—QoS is enabled on the device in Basic mode.
- **Advanced**—QoS is enabled on the device in Advanced mode.

STEP 3 Select **Port/LAG** and click **GO** to display/modify all ports/LAGs on the device and their CoS information.

The following fields are displayed for all ports/LAGs:

- **Interface**—Type of interface.
- **Default CoS**—Default VPT value for incoming packets that do not have a VLAN Tag. The default CoS is 0. The default is only relevant for untagged frames and only if the system is in Basic mode and Trust CoS is selected in the Global Settings page.

Select **Restore Defaults** to restore the factory CoS default setting for this interface.

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

To set QoS on an interface, select it, and click **Edit**.

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).

STEP 2 Click **Apply**. The interface default CoS value is saved to Running Configuration file.

Configuring QoS Queues

The device supports 4 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 there are a maximum of four queues possible and all four queues are WRR and the default weights are used, queue 1 receives 1/15 of the bandwidth (assuming all queues are saturated and there 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 or Queue 8 (the highest priority queue) and going to the next lower queue when each queue is completed.

When the queuing mode is Weighted Round Robin, queues are serviced until their quota has been used up and then another queue is serviced.

It is also possible to assign some of the lower queues to WRR, while keeping some of the higher queues in strict priority. In this case traffic for the 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**.

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 is the default CoS/802.1p priority assigned to the ingress ports.

The following table describes the default mapping when there are 4 queues:

802.1p Values (0-7, 7 being the highest)	Queue (4 queues 1-4, 4 being the highest priority)	Notes
0	1	Background
1	1	Best Effort
2	2	Excellent Effort
3	3	Critical Application - LVS phone SIP

802.1p Values (0-7, 7 being the highest)	Queue (4 queues 1-4, 4 being the highest priority)	Notes
4	3	Video
5	4	Voice - Cisco IP phone default
6	4	Interwork Control - LVS phone RTP
7	4	Network Control

By changing the CoS/802.1p to Queue mapping (CoS/802.1p to Queue) and the Queue schedule method and bandwidth allocation (Queue page), it is possible to achieve the desired quality of service in a network.

The CoS/802.1p to Queue mapping is applicable only if one of the following exists:

- The device is in QoS Basic mode and CoS/802.1p trusted mode
- The device is in QoS Advanced mode and the packets belong to flows that are CoS/802.1p trusted

Queue 1 has the lowest priority, queue 4 or 8 has the highest priority.

To map CoS values to egress queues:

STEP 1 Click **Quality of Service** > **General** > **CoS/802.1p to Queue**.

STEP 2 Enter the parameters.

- **802.1p—**Displays the 802.1p priority tag values to be assigned to an egress queue, where 0 is the lowest and 7 is the highest priority.
- **Output Queue—**Select the egress queue to which the 802.1p priority is mapped. Either four or eight egress queues are supported, where Queue 4 or Queue 8 is the highest priority egress queue and Queue 1 is the lowest priority.

STEP 3 For each 802.1p priority, select the Output Queue to which it is mapped.

STEP 4 Click **Apply**. 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 values to egress queues. The DSCP to Queue Table determines the egress queues of the incoming IP packets based on their DSCP values. The original VPT (VLAN Priority Tag) of the packet is unchanged.

By simply changing the DSCP to Queue mapping and the Queue schedule method and bandwidth allocation, it is possible to achieve the desired quality of services in a network.

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

- The device is in QoS Basic mode and DSCP is the trusted mode, or
- The device is in QoS Advanced mode and the packets belongs to flows that is DSCP trusted

Non-IP packets are always classified to the best-effort queue.

The following tables describe the default DSCP to queue mapping for a 4-queue system:

DSCP	63	55	47	39	31	23	15	7
Queue	3	3	4	3	3	2	1	1
DSCP	62	54	46	38	30	22	14	6
Queue	3	3	4	3	3	2	1	1
DSCP	61	53	45	37	29	21	13	5
Queue	3	3	4	3	3	2	1	1
DSCP	60	52	44	36	28	20	12	4
Queue	3	3	4	3	3	2	1	1
DSCP	59	51	43	35	27	19	11	3
Queue	3	3	4	3	3	2	1	1
DSCP	58	50	42	34	26	18	10	2
Queue	3	3	4	3	3	2	1	1
DSCP	57	49	41	33	25	17	9	1
Queue	3	3	4	3	3	2	1	1
DSCP	56	48	40	32	24	16	8	0
Queue	3	3	4	3	3	2	1	1

To map DSCP to queues:

STEP 1 Click **Quality of Service** > **General** > **DSCP to Queue**.

The DSCP to Queue page contains **Ingress DSCP**. It displays the DSCP value in the incoming packet and its associated class.

STEP 2 Select the **Output Queue** (traffic forwarding queue) to which the DSCP value is mapped.

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

Configuring Bandwidth

The Bandwidth page enables users to define two values, Ingress Rate Limit and Egress Shaping Rate, which 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 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**.

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.
- **Ingress Committed Burst Size (CBS)**—Enter the maximum burst size of data for the ingress interface in bytes of data. This amount can be sent even if it temporarily increases the bandwidth beyond the allowed limit. This field is only available if the interface is a port.
- **Egress Shaping Rate**—Select to enable egress shaping on the interface.

- **Committed Information Rate (CIR)**—Enter the maximum bandwidth for the egress interface.
- **Egress 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 written to the Running Configuration file.

Configuring Egress Shaping per Queue

In addition to limiting transmission rate per port, which is done in the Bandwidth page, the device can limit the transmission rate of selected egressing frames on a per-queue per-port basis. Egress rate limiting is performed by shaping the output load.

The device limits all frames except for management frames. Any frames that 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 displays the rate limit and burst size for each queue.

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

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

This page enables shaping the egress for up to eight queues on each interface.

STEP 4 Select the **Interface**.

STEP 5 For each queue that is required, enter the following fields:

- **Enable Shaping**—Select to enable egress shaping on this queue.
- **Committed Information Rate (CIR)**—Enter the maximum rate (CIR) in Kbits per second (Kbps). CIR is the average maximum amount of data that can be sent.

- **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 written to the Running Configuration file.

VLAN Ingress Rate Limit

NOTE The VLAN Rate Limit feature is not available when the device is in Layer 3 mode.

Rate limiting per VLAN, performed in the VLAN Ingress Rate Limit page, enables traffic limiting on VLANs. When VLAN ingress rate limiting is configured, it limits aggregate traffic from all the ports on the device.

The following constraints apply to rate limiting per VLAN:

- It has lower precedence than any other traffic policing defined in the system. For example, if a packet is subject to QoS rate limits but is also subject to VLAN rate limiting, and the rate limits conflict, the QoS rate limits take precedence.
- It is applied at the device level and within the device at the packet processor level. If there is more than one packet processor on the device, the configured VLAN rate limit value is applied to each of the packet processors, independently. Devices with up to 24 ports have a single packet processor, while devices of 48 ports or more have two packet processors.

To define the VLAN ingress rate limit:

STEP 1 Click **Quality of Service** > **General** > **VLAN Ingress Rate Limit**.

This page displays the VLAN Ingress Rate Limit Table.

STEP 2 Click **Add**.

STEP 3 Enter the parameters.

- **VLAN ID**—Select a VLAN.
- **Committed Information Rate (CIR)**—Enter the average maximum amount of data that can be accepted into the VLAN in Kilobytes per second.

- **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. Cannot be entered for LAGs.

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

TCP Congestion Avoidance

The TCP Congestion Avoidance page enables activating a TCP congestion avoidance algorithm. The algorithm breaks up or avoids TCP global synchronization in a congested node, where the congestion is due to various sources sending packets with the same byte count.

To configure TCP congestion avoidance:

STEP 1 Click **Quality of Service** > **General** > **TCP Congestion Avoidance**.

STEP 2 Click **Enable** to enable TCP congestion avoidance, and click **Apply**.

QoS Basic Mode

In QoS Basic mode, a specific domain in the network can be defined as trusted. Within that domain, packets are marked with 802.1p priority and/or DSCP to signal the type of service they require. Nodes within the domain use these fields to assign the packet to a specific output queue. The initial packet classification and marking of these fields is done in the ingress of the trusted domain.

Workflow to Configure Basic QoS Mode

To configure Basic QoS mode, perform the following:

1. Select Basic mode for the system by using the QoS Properties page.
2. Select the trust-behavior using the Global Setting page. The device supports CoS/802.1p trusted mode and DSCP trusted mode. CoS/802.1p trusted mode uses the 802.1p priority in the VLAN tag. DSCP trusted mode use the DSCP value in the IP header.

If there is any port that, as an exception, should not trust the incoming CoS mark, disable the QoS state on that port using the Interface Settings page.

Enable or disable the global selected trusted mode at the ports by using the Interface Settings page. If a port is disabled without trusted mode, all its ingress packets are forward in best effort. It is recommended that you disable the trusted mode at the ports where the CoS/802.1p and/or DSCP values in the incoming packets are not trustworthy. Otherwise, it might negatively affect the performance of your network

Configuring Global Settings

The Global Settings page contains information for enabling Trust on the device (see the Trust Mode field below). This configuration is active when the QoS mode is Basic mode. Packets entering a QoS domain are classified at the edge of the QoS domain.

To define the Trust configuration:

STEP 1 Click **Quality of Service** > **QoS Basic Mode** > **Global Settings**.

STEP 2 Select the **Trust Mode** while the device is in Basic mode. If a packet CoS level and DSCP tag are mapped to separate queues, the Trust mode determines the queue to which the packet is assigned:

- **CoS/802.1p**—Traffic is mapped to queues based on the VPT field in the VLAN tag, or based on the per-port default CoS/802.1p value (if there is no VLAN tag on the incoming packet), the actual mapping of the VPT to queue can be configured in the mapping CoS/802.1p to Queue page.
- **DSCP**—All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured in the DSCP to Queue page. If traffic is not IP traffic, it is mapped to the best effort queue.
- **CoS/802.1p-DSCP**—Either CoS/802.1p or DSCP whichever has been set.

STEP 3 Select **Override Ingress DSCP** to override the original DSCP values in the incoming packets with the new values according to the DSCP Override Table. When Override Ingress DSCP is enabled, the device uses the new DSCP values for egress queueing. It also replaces the original DSCP values in the packets with the new DSCP values.

NOTE The frame is mapped to an egress queue using the new, rewritten value, and not by the original DSCP value.

STEP 4 If **Override Ingress DSCP** was enabled, click **DSCP Override Table** to reconfigure DSCP.

DSCP In displays the DSCP value of the incoming packet that needs to be re-marked to an alternative value.

STEP 5 Select the **DSCP Out** value to indicate the outgoing value is mapped.

STEP 6 Click **Apply**. The Running Configuration file is updated with the new DSCP values.

Interface QoS Settings

The Interface Settings page enables configuring QoS on each port of the device, as follows:

QoS State Disabled on an Interface—All inbound traffic on the port is mapped to the best effort queue and no classification/prioritization takes place.

QoS State of the Port is Enabled—Port prioritize traffic on ingress is based on the system wide configured trusted mode, which is either CoS/802.1p trusted mode or DSCP trusted mode.

To enter QoS settings per interface:

STEP 1 Click **Quality of Service** > **QoS Basic Mode** > **Interface Settings**.

STEP 2 Select **Port** or **LAG** to display the list of ports or LAGs.

QoS State displays whether QoS is enabled on the interface.

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

STEP 4 Select the **Port** or **LAG** interface.

STEP 5 Click to enable or disable **QoS State** for this interface.

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

QoS Advanced Mode

Frames that match an ACL and were permitted entrance are implicitly labeled with the name of the ACL that permitted their entrance. Advanced mode QoS actions can then be applied to these flows.

In QoS advanced mode, the device uses policies to support per flow QoS. A policy and its components have the following characteristics and relationships:

- A policy contains one or more class maps.
- A class map defines a flow with one or more associating ACLs. Packets that match only ACL rules (ACE) in a class map with Permit (forward) action are considered belonging to the same flow, and are subjected to the same quality of services. Thus, a policy contains one or more flows, each with a user defined QoS.
- The QoS of a class map (flow) is enforced by the associating policer. There are two type of policers, single policer and aggregate policer. Each policer is configured with a QoS specification. A single policer applies the QoS to a single class map, and thus to a single flow, based on the policer QoS specification. An aggregate policer applies the QoS to one or more class maps, and thus one or more flows. An aggregate policer can support class maps from different policies.
- Per flow QoS are applied to flows by binding the policies to the desired ports. A policy and its class maps can be bound to one or more ports, but each port is bound with at most one policy.

Notes:

- Single policer and aggregation policer are available when the device is in Layer 2 mode.
- An ACL can be configured to one or more class maps regardless of policies.
- A class map can belong to only one policy.
- When a class map using single policer is bound to multiple ports, each port has its own instance of single policer; each applying the QoS on the class map (flow) at a port independent of each other.
- An aggregate policer applies the QoS to all its flow(s) in aggregation regardless of policies and ports.

Advanced QoS settings consist of three parts:

- Definitions of the rules to match. All frames matching a single group of rules are considered to be a *flow*.
- Definition of the actions to be applied to frames in each flow that match the rules.
- Binding the combinations of rules and action to one or more interfaces.

Workflow to Configure Advanced QoS Mode

To configure Advanced QoS mode, perform the following:

1. Select Advanced mode for the system by using the QoS Properties page*.* Select the Trust Mode using the Global Settings page. If a packet CoS level and DSCP tag are mapped to separate queues, the Trust mode determines the queue to which the packet is assigned:
    - If internal DSCP values are different from those used on incoming packets, map the external values to internal values by using the Out-of-Profile DSCP Mapping page. This in turn opens the DSCP Remarking page.
2. Create ACLs, as described in Create ACL Workflow.
3. If ACLs were defined, create class maps and associate the ACLs with them by using the Class Mapping page.
4. Create a policy using the Policy Table page, and associate the policy with one or more class maps using the Policy Class Map page. You can also specify the QoS, if needed, by assigning a policer to a class map when you associate the class map to the policy.
    - **Single Policer—**Create a policy that associates a class map with a single policer by using the Policy Table page and the Class Mapping page. Within the policy, define the single policer.
    - **Aggregate Policer—**Create a QoS action for each flow that sends all matching frames to the same policer (aggregate policer) by using the Aggregate Policer page. Create a policy that associates a class map with the aggregate policer by using the Policy Table page.
5. Bind the policy to an interface by using the Policy Binding page.

Configuring Global Settings

The Global Settings page contains information for enabling Trust on the device. Packets entering a QoS domain are classified at the edge of the QoS domain.

To define the Trust configuration:

STEP 1 Click **Quality of Service** > **QoS Advanced Mode** > **Global Settings**.

STEP 2 Select the **Trust Mode** while the device is in Advanced mode. If a packet CoS level and DSCP tag are mapped to separate queues, the Trust mode determines the queue to which the packet is assigned:

- **CoS/802.1p—**Traffic is mapped to queues based on the VPT field in the VLAN tag, or based on the per-port default CoS/802.1p value (if there is no VLAN tag on the incoming packet), the actual mapping of the VPT to queue can be configured in the mapping CoS/802.1p to Queue page.
- **DSCP—**All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured in the DSCP to Queue page. If traffic is not IP traffic, it is mapped to the best effort queue.
- **CoS/802.1p-DSCP—**Select to use Trust CoS mode for non-IP traffic and Trust DSCP for IP traffic.

STEP 3 Select the default Advanced mode QoS trust mode (either trusted or untrusted) for interfaces in the **Default Mode Status** field. This provides basic QoS functionality on Advanced QoS, so that you can trust CoS/DSCP on Advanced QoS by default (without having to create a policy).

In **QoS Advanced Mode**, when the Default Mode Status is set to Not Trusted, the default CoS values configured on the interface is ignored and all the traffic goes to queue 1. See the Quality of Service > QoS Advanced Mode > Global Settings page for details.

If you have a policy on an interface then the Default Mode is irrelevant, the action is according to the policy configuration and unmatched traffic is dropped.

STEP 4 Select **Override Ingress DSCP** to override the original DSCP values in the incoming packets with the new values according to the DSCP Override Table. When Override Ingress DSCP is enabled, the device uses the new DSCP values for egress queueing. It also replaces the original DSCP values in the packets with the new DSCP values.

NOTE The frame is mapped to an egress queue using the new, rewritten value, and not by the original DSCP value.

STEP 5 If **Override Ingress DSCP** was enabled, click **DSCP Override Table** to reconfigure DSCP. See the DSCP Override Table page for details.

Configuring Out-of-Profile DSCP Mapping

When a policer is assigned to a class maps (flows), you can specify the action to take when the amount of traffic in the flow(s) exceeds the QoS-specified limits. The portion of the traffic that causes the flow to exceed its QoS limit is referred to as *out-of-profile packets*.

If the exceed action is Out of Profile DSCP, the device remaps the original DSCP value of the out-of-profile IP packets with a new value based on the Out of Profile DSCP Mapping Table. The device uses the new values to assign resources and the egress queues to these packets. The device also physically replaces the original DSCP value in the out of profile packets with the new DSCP value.

To use the out-of-profile DSCP exceed action, remap the DSCP value in the Out Of Profile DSCP Mapping Table. Otherwise the action is null, because the DSCP value in the table remaps the packets to itself by factory default.

This feature changes the DSCP tags for incoming traffic switched between trusted QoS domains. Changing the DSCP values used in one domain, sets the priority of that type of traffic to the DSCP value used in the other domain to identify the same type of traffic.

These settings are active when the system is in the QoS basic mode, and once activated they are active globally.

For example: Assume that there are three levels of service: Silver, Gold, and Platinum and the DSCP incoming values used to mark these levels are 10, 20, and 30 respectively. If this traffic is forwarded to another service provider that has the same three levels of service, but uses DSCP values 16, 24, and 48, **Out of Profile DSCP Mapping** changes the incoming values as they are mapped to the outgoing values.

To map DSCP values:

STEP 1 Click **Quality of Service > QoS Advanced Mode > Out of Profile DSCP Mapping.** This page enables setting the change-the-DSCP-value of traffic entering or leaving the device.

DSCP In displays the DSCP value of the incoming packet that needs to be re-marked to an alternative value.

STEP 2 Select the **DSCP Out** value to where the incoming value is mapped.

STEP 3 Click **Apply.** The Running Configuration file is updated with the new DSCP Mapping table.

Defining Class Mapping

A Class Map defines a traffic flow with ACLs (Access Control Lists). A MAC ACL, IP ACL, and IPv6 ACL can be combined into a class map. Class maps are configured to match packet criteria on a match-all or match-any basis. They are matched to packets on a first-fit basis, meaning that the action associated with the first-matched class map is the action performed by the system. Packets that matches the same class map are considered to belong to the same flow.

NOTE Defining class maps does not have any effect on QoS; it is an interim step, enabling the class maps to be used later.

If more complex sets of rules are needed, several class maps can be grouped into a super-group called a policy (see **Configuring a Policy**).

The Class Mapping page shows the list of defined class maps and the ACLs comprising each, and enables you to add/delete class maps.

To define a Class Map:

STEP 1 Click **Quality of Service** > **QoS Advanced Mode** > **Class Mapping**.

This page displays the already-defined class maps.

STEP 2 Click **Add**.

A new class map is added by selecting one or two ACLs and giving the class map a name. If a class map has two ACLs, you can specify that a frame must match both ACLs, or that it must match either one or both of the ACLs selected.

STEP 3 Enter the parameters.

- **Class Map Name—**Enter the name of a new class map.
- **Match ACL Type—**The criteria that a packet must match in order to be considered to belong to the flow defined in the class map. The options are:
  - *IP*—A packet must match either of the IP based ACLs in the class map.
  - *MAC*—A packet must match the MAC based ACL in the class map.
  - *IP and MAC*—A packet must match the IP based ACL and the MAC based ACL in the class map.
  - *IP or MAC*—A packet must match either the IP based ACL or the MAC based ACL in the class map.
- **IP—**Select the IPv4 based ACL or the IPv6 based ACL for the class map.
- **MAC—**Select the MAC based ACL for the class map.
- **Preferred ACL—**Select whether packets are first matched to an IP-based ACL or a MAC-based ACL.

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

QoS Policers

NOTE QoS policers are not supported on Sx500 devices in Layer 3 system mode. They are always supported on SG500X devices.

You can measure the rate of traffic that matches a pre-defined set of rules, and to enforce limits, such as limiting the rate of file-transfer traffic that is allowed on a port.

This can be done by using the ACLs in the class map(s) to match the desired traffic, and by using a policer to apply the QoS on the matching traffic.

A policer is configured with a QoS specification. There are two kinds of policers:

- **Single (Regular) Policer—**A single policer applies the QoS to a single class map, and to a single flow based on the policer's QoS specification. When a class map using single policer is bound to multiple ports, each port has its own instance of single policer; each applying the QoS on the class map (flow) at ports that are otherwise independent of each other. A single policer is created in the Policy Table page.

- **Aggregate Policer—**An aggregate policer applies the QoS to one or more class maps, and one or more flows. An aggregation policer can support class maps from different policies. An aggregate policer applies QoS to all its flow(s) in aggregation regardless of policies and ports. An aggregate policer is created in the Aggregate Policer page.

  An aggregate policer is defined if the policer is to be shared with more than one class. Policers on a port cannot be shared with other policers in another device.

Each policer is defined with its own QoS specification with a combination of the following parameters:

- A maximum allowed rate, called a Committed Information Rate (CIR), measured in Kbps.
- An amount of traffic, measured in bytes, called a Committed Burst Size (CBS). This is traffic that is allowed to pass as a temporary burst even if it is above the defined maximum rate.
- An action to be applied to frames that are over the limits (called out-of-profile traffic), where such frames can be passed as is, dropped, or passed, but remapped to a new DSCP value that marks them as lower-priority frames for all subsequent handling within the device.

Assigning a policer to a class map is done when a class map is added to a policy. If the policer is an aggregate policer, you must create it using the Aggregate Policer page.

Defining Aggregate Policers

An aggregate policer applies the QoS to one or more class maps, therefore one or more flows. An aggregation policer can support class maps from different policies and applies the QoS to all its flow(s) in aggregation regardless of policies and ports.

NOTE The device supports aggregate policers and single policers only when operating in Layer 2 mode in devices that support a separate Layer 2 system mode.

To define an aggregate policer:

STEP 1 Click **Quality of Service** > **QoS Advanced Mode** > **Aggregate Policer**.

This page displays the existing aggregate policers.

STEP 2 Click **Add**.

STEP 3 Enter the parameters.

- **Aggregate Policer Name—**Enter the name of the Aggregate Policer.
- **Ingress Committed Information Rate** (CIR)—Enter the maximum bandwidth allowed in bits per second. See the description of this in the Bandwidth page.
- **Ingress Committed Burst Size (CBS)**—Enter the maximum burst size (even if it goes beyond the CIR) in bytes. See the description of this in the Bandwidth page.
- **Exceed Action—**Select the action to be performed on incoming packets that exceed the CIR. Possible values are:
  - *Forward*—Packets exceeding the defined CIR value are forwarded.
  - *Drop*—Packets exceeding the defined CIR value are dropped.
  - *Out of Profile DSCP*—The DSCP values of packets exceeding the defined CIR value are remapped to a value based on the Out Of Profile DSCP Mapping Table.

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

Configuring a Policy

The Policy Table Map page displays the list of advanced QoS polices defined in the system. The page also allows you to create and delete polices. Only those policies that are bound to an interface are active (see Policy Binding page).

Each policy consists of:

- One or more class maps of ACLs which define the traffic flows in the policy.
- One or more aggregates that applies the QoS to the traffic flows in the policy.

After a policy has been added, class maps can be added by using the Policy Table page.

To add a QoS policy:

STEP 1 Click **Quality of Service** > **QoS Advanced Mode** > **Policy Table**.

This page displays the list of defined policies.

STEP 2 Click **Policy Class Map Table** to display the Policy Class Maps page.
-or
Click **Add** to open the Add Policy Table page.

STEP 3 Enter the name of the new policy in the **New Policy Name** field.

STEP 4 Click **Apply**. The QoS policy profile is added, and the Running Configuration file is updated.

Policy Class Maps

One or more class maps can be added to a policy. A class map defines the type of packets that are considered to belong to the same traffic flow.

NOTE You cannot configure a policer to a class map when the device is operating in Layer 3 mode. The device supports policers only in Layer 2 mode.

To add a class map to a policy:

STEP 1 Click **Quality of Service** > **QoS Advanced Mode** > **Policy Class Maps**.

STEP 2 Select a policy in the Filter, and click **Go**. All class maps in that policy are displayed.

STEP 3 To add a new class map, click **Add**.

STEP 4 Enter the parameters.

- **Policy Name**—Displays the policy to which the class map is being added.
- **Class Map Name**—Select an existing class map to be associated with the policy. Class maps are created in the Class Mapping page.
- **Action Type**—Select the action regarding the ingress CoS/802.1p and/or DSCP value of all the matching packets.
  - *Use default trust mode*—Ignore the ingress CoS/802.1p and/or DSCP value. The matching packets are sent as best effort.

  - *Always Trust*—If this option is selected, the device trusts the CoS/802.1p and DSCP of the matching packet. If a packet is an IP packet, the device puts the packet in the egress queue based on its DSCP value and the DSCP to Queue Table. Otherwise, the egress queue of the packet is based on the packet's CoS/802.1p value and the CoS/802.1p to Queue Table.
  - *Set*—If this option is selected, use the value entered in the **New Value** box to determine the egress queue of the matching packets as follows:

    If the new value (0..7) is a CoS/802.1p priority, use the priority value and the CoS/802.1p to Queue Table to determine the egress queue of all the matching packets.

    If the new value (0..63) is a DSCP, use the new DSCP and the DSCP to Queue Table to determine the egress queue of the matching IP packets.

    Otherwise, use the new value (1..8) as the egress queue number for all the matching packets.

- **Police Type**—Available in Layer 2 system mode only. Select the policer type for the policy. The options are:
  - *None*—No policy is used.
  - *Single*—The policer for the policy is a single policer.
  - *Aggregate*—The policer for the policy is an aggregate policer.
- **Aggregate Policer**—Available in Layer 2 system mode only. If **Police Type** is *Aggregate*, select a previously-defined (in the Aggregate Policer page) aggregate policer.

If **Police Type** is *Single*, enter the following QoS parameters:

- **Ingress Committed Information Rate (CIR)**—Enter the CIR in Kbps. See a description of this in the Bandwidth page.
- **Ingress Committed Burst Size (CBS)**—Enter the CBS in bytes. See a description of this in the Bandwidth page.
- **Exceed Action**—Select the action assigned to incoming packets exceeding the CIR. The options are:
  - *None*—No action.
  - *Drop*—Packets exceeding the defined CIR value are dropped.

- *Out of Profile DSCP*—IP packets exceeding the defined CIR are forwarding with a new DSCP derived from the Out Of Profile DSCP Mapping Table.

STEP 5 Click **Apply**.

Policy Binding

The Policy Binding page shows which policy profile is bound and to which port. When a policy profile is bound to a specific port, it is active on that port. Only one policy profile can be configured on a single port, but a single policy can be bound to more than one port.

When a policy is bound to a port, it filters and applies QoS to ingress traffic that belongs to the flows defined in the policy. The policy does not apply to traffic egress to the same port.

To edit a policy, it must first be removed (unbound) from all those ports to which it is bound.

NOTE It is possible to either bind a port to a policy or to an ACL but both cannot be bound.

To define policy binding:

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

STEP 2 Select a **Policy Name** and **Interface Type** if required.

STEP 3 Click **Go**. The policy is selected.

STEP 4 Select the following for the policy/interface:

- **Binding**—Select to bind the policy to the interface.
- **Permit Any**—Select to forward packets on the interface if they do not match any policy.

  NOTE Permit Any can be defined only if IP Source Guard is not activated on the interface.

STEP 5 Click **Apply**. The QoS policy binding is defined, and the Running Configuration file is updated.

Managing QoS Statistics

From these pages you can manage the Single Policer, Aggregated Policer, and view queues statistics.

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 Single Policer Statistics

The Single Policer Statistics page indicates the number of in-profile and out-of-profile packets that are received from an interface that meet the conditions defined in the class map of a policy.

NOTE This page is not displayed when the device is in Layer 3 mode.

To view policer statistics:

STEP 1 Click **Quality of Service** > **QoS Statistics** > **Single Policer Statistics**.

This page displays the following fields:

- **Interface—**Statistics are displayed for this interface.
- **Policy—**Statistics are displayed for this policy.
- **Class Map—**Statistics are displayed for this class map.
- **In-Profile Bytes—**Number of in-profile bytes received.
- **Out-of-Profile Bytes—**Number of out-profile bytes received.

STEP 2 Click **Add.**

STEP 3 Enter the parameters.

- **Interface—**Select the interface for which statistics are accumulated.
- **Policy Name—**Select the policy name.
- **Class Map Name—**Select the class name.

STEP 4 Click **Apply**. An additional request for statistics is created and the Running Configuration file is updated.

Viewing Aggregated Policer Statistics

To view aggregated policer statistics:

STEP 1 Click **Quality of Service** > **QoS Statistics** > **Aggregate Policer Statistics**.

This page displays the following fields:

- **Aggregate Policer Name—**Policer on which statistics are based.
- **In-profile bytes—**Number of in-profile packets that were received.
- **Out-of-profile bytes—**Number of out-of-profile packets that were received.

STEP 2 Click **Add**.

STEP 3 Select an **Aggregate Policer Name**, one of the previously-created Aggregate Policers for which statistics are displayed.

STEP 4 Click **Apply**. An additional request for statistics is created, and the Running Configuration file is updated.

Viewing Queues Statistics

The Queues Statistics page displays queue statistics, including statistics of forwarded and dropped packets, based on interface, queue, and drop precedence.

To view Queues Statistics:

STEP 1 Click **Quality of Service** > **QoS Statistics** > **Queues Statistics**.

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.**

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.

26

SNMP

This section describes the Simple Network Management Protocol (SNMP) feature that provides a method for managing network devices.

It covers the following topics:

- **SNMP Versions and Workflow**
- **Model OIDs**
- **SNMP Engine ID**
- **Configuring SNMP Views**
- **Creating SNMP Groups**
- **Managing SNMP Users**
- **Defining SNMP Communities**
- **Defining Trap Settings**
- **Notification Recipients**
- **SNMP Notification Filters**

SNMP Versions and Workflow

The device functions as SNMP agent and supports SNMPv1, v2, and v3. It also reports system events to trap receivers using the traps defined in the supported MIBs (Management Information Base).

SNMPv1 and v2

To control access to the system, a list of community entries is defined. Each community entry consists of a *community string* and its access privilege. The system responds only to SNMP messages specifying the community which has the correct permissions and correct operation.

SNMP agents maintain a list of variables that are used to manage the device. These variables are defined in the *Management Information Base* (MIB).

NOTE Due to the security vulnerabilities of other versions, it is recommended to use SNMPv3.

SNMPv3

In addition to the functionality provided by SNMPv1 and v2, SNMPv3 applies access control and new trap mechanisms to SNMPv1 and SNMPv2 PDUs. SNMPv3 also defines a User Security Model (USM) that includes:

- **Authentication—**Provides data integrity and data origin authentication.
- **Privacy—**Protects against disclosure message content. *Cipher Block-Chaining* (CBC-DES) is used for encryption. Either authentication alone can be enabled on an SNMP message, or both authentication and privacy can be enabled on an SNMP message. However, privacy cannot be enabled without authentication.
- **Timeliness—**Protects against message delay or playback attacks. The SNMP agent compares the incoming message time stamp to the message arrival time.
- **Key Management—**Defines key generation, key updates, and key use. The device supports SNMP notification filters based on *Object IDs* (OID). OIDs are used by the system to manage device features.

SNMP Workflow

NOTE For security reasons, SNMP is disabled by default. Before you can manage the device via SNMP, you must turn on SNMP on the Security >TCP/UDP Services page.

The following is the recommended series of actions for configuring SNMP:

If you decide to use SNMPv1 or v2:

STEP 1 Navigate to the SNMP -> Communities page and click **Add**. The community can be associated with access rights and a view in Basic mode or with a group in Advanced mode. There are two ways to define access rights of a community:

- **Basic mode**—The access rights of a community can configure with Read Only, Read Write, or SNMP Admin. In addition, you can restrict the access to the community to only certain MIB objects by selecting a view (defined in the Views page).
- **Advanced Mode**—The access rights of a community are defined by a group (defined in the Groups page). You can configure the group with a specific security model. The access rights of a group are Read, Write, and Notify.

STEP 2 Choose whether to restrict the SNMP management station to one address or allow SNMP management from all addresses. If you choose to restrict SNMP management to one address, then input the address of your SNMP Management PC in the IP Address field.

STEP 3 Input the unique community string in the Community String field.

STEP 4 Optionally, enable traps by using the Trap Settings page.

STEP 5 Optionally, define a notification filter(s) by using the Notification Filter page.

STEP 6 Configure the notification recipients on the Notification Recipients SNMPv1,2 page.

If you decide to use SNMPv3:

STEP 1 Define the SNMP engine by using the Engine ID page. Either create a unique Engine ID or use the default Engine ID. Applying an Engine ID configuration clears the SNMP database.

STEP 2 Optionally, define SNMP view(s) by using the Views page. This limits the range of OIDs available to a community or group.

STEP 3 Define groups by using the Groups page.

STEP 4 Define users by using the SNMP Users page, where they can be associated with a group. If the SNMP Engine ID is not set, then users may not be created.

STEP 5 Optionally, enable or disable traps by using the Trap Settings page.

STEP 6 Optionally, define a notification filter(s) by using the Notification Filter page.

STEP 7 Define a notification recipient(s) by using the Notification Recipients SNMPv3 page.

Supported MIBs

For a list of supported MIBs, visit the following URL and navigate to the download area listed as **Cisco MIBS**:

www.cisco.com/cisco/software/navigator.html

Model OIDs

The following are the device model *Object IDs* (OIDs):

Model Name	Description	Object ID
SG300-10	8 GE ports, and 2 special-purpose combo ports (GE/SFP)	9.6.1.83.10.1
SG300-10MP	8 GE ports, and 2 special-purpose combo ports (GE/SFP)	9.6.1.83.10.3
SG300-10P	8 GE ports, and 2 special-purpose combo ports (GE/SFP)	9.6.1.83.10.2
SG300-20	16 GE ports, and 4 special purpose ports - 2 uplinks and 2 combo ports	9.6.1.83.20.1
SG300-28	24 GE ports, and 4 special-purpose ports - 2 uplinks and 2 combo-ports	9.6.1.83.28.1
SG300-28P	24 GE ports, and 4 special-purpose ports - 2 uplinks and 2 combo-ports.	9.6.1.83.28.2
SG300-52	48 GE ports, and 4 special-purpose ports - 2 uplinks and 2 combo-ports	9.6.1.83.52.1
SF300-08	8 FE ports.	9.6.1.82.08.4
SF302-08	8 FE ports plus 2 GE ports	9.6.1.82.08.1

Model Name	Description	Object ID
SF302-08MP	8 FE ports plus 2 GE ports	9.6.1.82.08.3
SF302-08P	8 FE ports plus 2 GE ports	9.6.1.82.08.2
SF300-24	24 FE ports plus 4 GE special-purpose ports - 2 uplinks and 2 combo-ports.	9.6.1.82.24.1
SF300-24P	24 FE ports plus 4 GE special-purpose ports - 2 uplinks and 2 combo-ports.	9.6.1.82.24.2
SF300-48	48 FE ports plus 4 GE special-purpose ports - 2 uplinks and 2 combo-ports	9.6.1.82.48.1
SF300-48P	48 FE ports plus 4 GE special-purpose ports - 2 uplinks and 2 combo-ports	9.6.1.82.48.2
SG300-52P	52-Port Gigabit PoE Managed Switch	9.6.1.83.52.2
SG300-52MP	52-Port Gigabit PoE Managed Switch	9.6.1.83.52.3
SG300-10SFP	10-Port Gigabit Managed SFP Switch	9.6.1.83.10.5
ESW2-350G-52	52-Port Gigabit Managed Switch	9.6.1.86.52.1
ESW2-350G-52DC	52-Port Gigabit Managed Switch	9.6.1.86.52.6
SF300-24MP	24-Port 10/100 PoE Managed Switch	9.6.1.82.24.3
SG300-28MP	28-Port Gigabit PoE Managed Switch	9.6.1.83.28.3
SF302-08P	8 FE ports plus 2 GE ports	9.6.1.82.08.2
SF302-08PP	8-Port 10/100 PoE Managed Switch	9.6.1.82.08.2
SF302-08MPP	8-Port 10/100 PoE Managed Switch	9.6.1.82.08.3
SG300-10PP	8-Port 10/100 PoE Managed Switch	9.6.1.83.10.2
SF300-24PP	8-Port 10/100 PoE Managed Switch	9.6.1.82.24.1
SG300-28PP	10-Port Gigabit PoE Managed Switch	9.6.1.83.28.2
SF300-24PP	24-Port 10/100 PoE Managed Switch	9.6.1.82.24.1
SG300-28PP	28-Port Gigabit PoE Managed Switch	9.6.1.83.28.2
SF300-48PP	48-Port 10/100 PoE Managed Switch	9.6.1.82.48.2

The private Object IDs are placed under: enterprises(1).cisco(9).otherEnterprises(6).ciscosb(1).switch001(101).

SNMP Engine ID

The Engine ID is used by SNMPv3 entities to uniquely identify them. An SNMP agent is considered an authoritative SNMP engine. This means that the agent responds to incoming messages (Get, GetNext, GetBulk, Set) and sends trap messages to a manager. The agent's local information is encapsulated in fields in the message.

Each SNMP agent maintains local information that is used in SNMPv3 message exchanges. The default SNMP Engine ID is comprised of the enterprise number and the default MAC address. This engine ID must be unique for the administrative domain, so that no two devices in a network have the same engine ID.

Local information is stored in four MIB variables that are read-only (snmpEngineId, snmpEngineBoots, snmpEngineTime, and snmpEngineMaxMessageSize).

CAUTION When the engine ID is changed, all configured users and groups are erased.

To define the SNMP engine ID:

STEP 1 Click **SNMP** > **Engine ID**.

STEP 2 Choose which to use for **Local Engine ID**.

- **Use Default**—Select to use the device-generated engine ID. The default engine ID is based on the device MAC address, and is defined per standard as:
  - *First 4 octets*—First bit = 1, the rest is the IANA enterprise number.
  - *Fifth octet*—Set to 3 to indicate the MAC address that follows.
  - *Last 6 octets*—MAC address of the device.
- **None**—No engine ID is used.
- **User Defined**—Enter the local device engine ID. The field value is a hexadecimal string **(range: 10 - 64)**. Each byte in the hexadecimal character strings is represented by two hexadecimal digits.

All remote engine IDs and their IP addresses are displayed in the Remote Engine ID table.

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

The Remote Engine ID table shows the mapping between IP addresses of the engine and Engine ID. To add the IP address of an engine ID:

STEP 4 Click **Add**. Enter the following fields:

- **Server Definition—**Select whether to specify the Engine ID server by IP address or name.
- **IP Version—**Select the supported IP format.
- **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.
- **Server IP Address/Name—**Enter the IP address or domain name of the log server.
- **Engine ID—**Enter the Engine ID.

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

Configuring SNMP Views

A view is a user-defined label for a collection of MIB subtrees. Each subtree ID is defined by the *Object ID* (OID) of the root of the relevant subtrees. Either well-known names can be used to specify the root of the desired subtree or an OID can be entered (see **Model OIDs**).

Each subtree is either included or excluded in the view being defined.

The Views page enables creating and editing SNMP views. The default views (Default, DefaultSuper) cannot be changed.

Views can be attached to groups in the Groups page or to a community which employs basic access mode through the Communities page.

To define SNMP views:

STEP 1 Click **SNMP** > **Views**.

STEP 2 Click **Add** to define new views.

STEP 3 Enter the parameters.

- **View Name—**Enter a view name between 0-30 characters)
- **Object ID Subtree—**Select the node in the MIB tree that is included or excluded in the selected SNMP view. The options to select the object are as follows:
    - *Select from list*—Enables you to navigate the MIB tree. Press the *Up* arrow to go to the level of the selected node's parent and siblings; press the *Down* arrow to descend to the level of the selected node's children. Click nodes in the view to pass from one node to its sibling. Use the scrollbar to bring siblings in view.
    - *User Defined*—Enter an OID not offered in the *Select from list* option.

STEP 4 Select or deselect **Include in view.** If this is selected, the selected MIBs are included in the view, otherwise they are excluded.

STEP 5 Click Apply.

STEP 6 In order to verify your view configuration, select the user-defined views from the **Filter: View Name** list. The following views exist by default:

- **Default**—Default SNMP view for read and read/write views.
- **DefaultSuper—**Default SNMP view for administrator views.

Other views can be added.

- **Object ID Subtree—**Displays the subtree to be included or excluded in the SNMP view.

- **Object ID Subtree View Type—**Displays whether the defined subtree is included or excluded in the selected SNMP view.

Creating SNMP Groups

In SNMPv1 and SNMPv2, a community string is sent along with the SNMP frames. The community string acts as a password to gain access to an SNMP agent. However, neither the frames nor the community string are encrypted. Therefore, SNMPv1 and SNMPv2 are not secure.

In SNMPv3, the following security mechanisms can be configured.

- **Authentication—**The device checks that the SNMP user is an authorized system administrator. This is done for each frame.
- **Privacy—**SNMP frames can carry encrypted data.

Thus, in SNMPv3, there are three levels of security:

- No security (No authentication and no privacy)
- Authentication (Authentication and no privacy)
- Authentication and privacy

SNMPv3 provides a means of controlling the content each user can read or write and the notifications they receive. A group defines read/write privileges and a level of security. It becomes operational when it is associated with an SNMP user or community.

NOTE To associate a non-default view with a group, first create the view in the Views page.

To create an SNMP group:

STEP 1 Click **SNMP** > **Groups.**

This page contains the existing SNMP groups and their security levels.

STEP 2 Click **Add**.

STEP 3 Enter the parameters.

- **Group Name—**Enter a new group name.

- **Security Model**—Select the SNMP version attached to the group, SNMPv1, v2, or v3.

Three types of views with various security levels can be defined. For each security level, select the views for Read, Write and Notify by entering the following fields:

- **Enable**—Select this field to enable the Security Level.
- **Security Level**—Define the security level attached to the group. SNMPv1 and SNMPv2 support neither authentication nor privacy. If SNMPv3 is selected, choose one of the following:
    - *No Authentication and No Privacy*—Neither the Authentication nor the Privacy security levels are assigned to the group.
    - *Authentication and No Privacy*—Authenticates SNMP messages, and ensures the SNMP message origin is authenticated but does not encrypt them.
    - *Authentication and Privacy*—Authenticates SNMP messages, and encrypts them.
- **View**—Associating a view with the read, write, and notify access privileges of the group limits the scope of the MIB tree to which the group has read, write, and notify access.
    - *View*—Select a previously-defined view for Read, Write and Notify.
    - *Read*—Management access is read-only for the selected view. Otherwise, a user or a community associated with this group is able to read all MIBs except those that control SNMP itself.
    - *Write*—Management access is write for the selected view. Otherwise, a user or a community associated with this group is able to write all MIBs except those that control SNMP itself.
    - *Notify*—Limits the available content of the traps to those included in the selected view. Otherwise, there is no restriction on the contents of the traps. This can only be selected for SNMPv3.

STEP 4 Click **Apply**. The SNMP group is saved to the Running Configuration file.

Managing SNMP Users

An SNMP user is defined by the login credentials (username, passwords, and authentication method) and by the context and scope in which it operates by association with a group and an Engine ID.

The configured user have the attributes of its group, having the access privileges configured within the associated view.

Groups enable network managers to assign access rights to a group of users instead of to a single user.

A user can only belong to a single group.

To create an SNMPv3 user, the following must first exist:

- An engine ID must first be configured on the device. This is done in the Engine ID page.
- An SNMPv3 group must be available. An SNMPv3 group is defined in the Groups page.

To display SNMP users and define new ones:

STEP 1 Click **SNMP** > **Users**.

This page contains existing users.

STEP 2 Click **Add.**

This page provides information for assigning SNMP access control privileges to SNMP users.

STEP 3 Enter the parameters.

- **User Name—**Enter a name for the user.
- **Engine ID—**Select either the local or remote SNMP entity to which the user is connected. Changing or removing the local SNMP Engine ID deletes the SNMPv3 User Database. To receive inform messages and request information, you must define both a local and remote user.
  - *Local*—User is connected to the local device.
  - *Remote IP Address*—User is connected to a different SNMP entity besides the local device. If the remote Engine ID is defined, remote devices receive inform messages, but cannot make requests for

information.

Enter the remote engine ID.

- **Group Name—**Select the SNMP group to which the SNMP user belongs. SNMP groups are defined in the Add Group page.

  NOTE Users, who belong to groups which have been deleted, remain, but they are inactive.

- **Authentication Method—**Select the Authentication method that varies according to the Group Name assigned. If the group does not require authentication, then the user cannot configure any authentication. The options are:
  - *None*—No user authentication is used.
  - *MD5 Password*—A password that is used for generating a key by the MD5 authentication method.
  - *SHA Password*—A password that is used for generating a key by the SHA (Secure Hash Algorithm) authentication method.
- **Authentication Password—**If authentication is accomplished by either a MD5 or a SHA password, enter the local user password in either **Encrypted** or **Plaintext**. Local user passwords are compared to the local database. and can contain up to 32 ASCII characters.
- **Privacy Method—**Select one of the following options:
  - *None*—Privacy password is not encrypted.
  - *DES*—Privacy password is encrypted according to the Data Encryption Standard (DES).
- **Privacy Password—**16 bytes are required (DES encryption key) if the DES privacy method was selected. This field must be exactly 32 hexadecimal characters. The **Encrypted** or **Plaintext** mode can be selected.

STEP 4 Click **Apply** to save the settings.

Defining SNMP Communities

Access rights in SNMPv1 and SNMPv2 are managed by defining communities in the Communities page. The community name is a type of shared password between the SNMP management station and the device. It is used to authenticate the SNMP management station.

Communities are only defined in SNMPv1 and v2 because SNMPv3 works with users instead of communities. The users belong to groups that have access rights assigned to them.

The Communities page associates communities with access rights, either directly (Basic mode) or through groups (Advanced mode):

- **Basic mode**—The access rights of a community can configure with Read Only, Read Write, or SNMP Admin. In addition, you can restrict the access to the community to only certain MIB objects by selecting a view (defined in the SNMP Views page).
- **Advanced Mode**—The access rights of a community are defined by a group (defined in the Groups page). You can configure the group with a specific security model. The access rights of a group are Read, Write, and Notify.

To define SNMP communities:

STEP 1 Click **SNMP** > **Communities**.

This page contains a table of configured SNMP communities and their properties.

STEP 2 Click **Add.**

This page enables network managers to define and configure new SNMP communities.

STEP 3 **SNMP Management Station**—Click **User Defined** to enter the management station IP address that can access the SNMP community. Click **All** to indicate that any IP device can access the SNMP community.

- **IP Version**—Select either IPv4 or IPv6.
- **IPv6 Address Type**—Select the supported 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 a VLAN or ISATAP.
- **IP Address**—Enter the SNMP management station IP address.
- **Community String**—Enter the community name used to authenticate the management station to the device.
- **Basic**—Select this mode for a selected community. In this mode, there is no connection to any group. You can only choose the community access level (Read Only, Read Write, or SNMP Admin) and, optionally, further qualify it for a specific view. By default, it applies to the entire MIB. If this is selected, enter the following fields:
    - *Access Mode*—Select the access rights of the community. The options are:

      Read Only—Management access is restricted to read-only. Changes cannot be made to the community.

      Read Write—Management access is read-write. Changes can be made to the device configuration, but not to the community.

      SNMP Admin—User has access to all device configuration options, as well as permissions to modify the community. SNMP Admin is equivalent to Read Write for all MIBs except for the SNMP MIBs. SNMP Admin is required for access to the SNMP MIBs.
    - *View Name*—Select an SNMP view (a collection of MIB subtrees to which access is granted).
- **Advanced**—Select this mode for a selected community.
    - *Group Name*—Select an SNMP group that determines the access rights.

STEP 4 Click **Apply**. The SNMP Community is defined, and the Running Configuration is updated.

Defining Trap Settings

The Trap Settings page enables configuring whether SNMP notifications are sent from the device, and for which cases. The recipients of the SNMP notifications can be configured in the Notification Recipients SNMPv1,2 page, or the Notification Recipients SNMPv3 page.

To define trap settings:

STEP 1 Click **SNMP** > **Trap Settings**.

STEP 2 Select **Enable** for **SNMP Notifications** to specify that the device can send SNMP notifications.

STEP 3 Select **Enable** for **Authentication Notifications** to enable SNMP authentication failure notification.

STEP 4 Click **Apply**. The SNMP Trap settings are written to the Running Configuration file.

Notification Recipients

Trap messages are generated to report system events, as defined in RFC 1215. The system can generate traps defined in the MIB that it supports.

Trap receivers (aka Notification Recipients) are network nodes where the trap messages are sent by the device. A list of notification recipients are defined as the targets of trap messages.

A trap receiver entry contains the IP address of the node and the SNMP credentials corresponding to the version that is included in the trap message. When an event arises that requires a trap message to be sent, it is sent to every node listed in the Notification Recipient Table.

The Notification Recipients SNMPv1,2 page and the Notification Recipients SNMPv3 page enable configuring the destination to which SNMP notifications are sent, and the types of SNMP notifications that are sent to each destination (traps or informs). The Add/Edit pop-ups enable configuring the attributes of the notifications.

An SNMP notification is a message sent from the device to the SNMP management station indicating that a certain event has occurred, such as a link up/down.

It is also possible to filter certain notifications. This can be done by creating a filter in the Notification Filter page and attaching it to an SNMP notification recipient. The notification filter enables filtering the type of SNMP notifications that are sent to the management station based on the OID of the notification that is about to be sent.

Defining SNMPv1,2 Notification Recipients

To define a recipient in SNMPv1,2:

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

This page displays recipients for SNMPv1,2.

STEP 2 Enter the following fields:

- **Informs IPv4 Source Interface—**Select the source interface whose IPv4 address will be used as the source IPv4 address in inform messages for communication with IPv4 SNMP servers.
- **Traps IPv4 Source Interface—**Select the source interface whose IPv6 address will be used as the source IPv6 address in trap messages for communication with IPv6 SNMP servers.
- **Informs IPv6 Source Interface—**Select the source interface whose IPv4 address will be used as the source IPv4 address in inform messages for communication with IPv4 SNMP servers.
- **Traps IPv6 Source Interface—**Select the source interface whose IPv6 address will be used as the source IPv6 address in trap messages for communication with IPv6 SNMP servers.

NOTE If the Auto option is selected, the system takes the source IP address from the IP address defined on the outgoing interface.

STEP 3 Click **Add.**

STEP 4 Enter the parameters.

- **Server Definition—**Select whether to specify the remote log server by IP address or name.
- **IP Version—**Select either IPv4 or IPv6.
- **IPv6 Address Type—**Select either *Link Local* or *Global*.

  - *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 a VLAN or ISATAP.
- **Recipient IP Address/Name**—Enter the IP address or server name of where the traps are sent.
- **UDP Port**—Enter the UDP port used for notifications on the recipient device.
- **Notification Type**—Select whether to send Traps or Informs. If both are required, two recipients must be created.
- **Timeout**—Enter the number of seconds the device waits before re-sending informs.
- **Retries**—Enter the number of times that the device resends an inform request.
- **Community String**—Select from the pull-down the community string of the trap manager. Community String names are generated from those listed in the Community page.
- **Notification Version**—Select the trap SNMP version.
  Either SNMPv1 or SNMPv2 may be used as the version of traps, with only a single version enabled at a time.
- **Notification Filter**—Select to enable filtering the type of SNMP notifications sent to the management station. The filters are created in the Notification Filter page.
- **Filter Name**—Select the SNMP filter that defines the information contained in traps (defined in the Notification Filter page).

STEP 5 Click **Apply**. The SNMP Notification Recipient settings are written to the Running Configuration file.

Defining SNMPv3 Notification Recipients

To define a recipient in SNMPv3:

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

This page displays recipients for SNMPv3.

- **Informs IPv4 Source Interface**—Select the source interface whose IPv4 address will be used as the source IPv4 address in inform messages for communication with IPv4 SNMP servers.
- **Traps IPv4 Source Interface**—Select the source interface whose IPv6 address will be used as the source IPv6 address in trap messages for communication with IPv6 SNMP servers.
- **Informs IPv6 Source Interface**—Select the source interface whose IPv4 address will be used as the source IPv4 address in inform messages for communication with IPv4 SNMP servers.
- **Traps IPv6 Source Interface**—Select the source interface whose IPv6 address will be used as the source IPv6 address in trap messages for communication with IPv6 SNMP servers.

STEP 2 Click **Add.**

STEP 3 Enter the parameters.

- **Server Definition**—Select whether to specify the remote log server by IP address or name.
- **IP Version**—Select either IPv4 or IPv6.
- **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 pull-down list.

- **Recipient IP Address/Name—**Enter the IP address or server name of where the traps are sent.
- **UDP Port—**Enter the UDP port used to for notifications on the recipient device.
- **Notification Type—**Select whether to send traps or informs. If both are required, two recipients must be created.
- Timeout—Enter the amount of time (seconds) the device waits before re-sending informs/traps. Timeout: Range 1-300, default 15
- Retries—Enter the number of times that the device resends an inform request. Retries: Range 1-255, default 3
- User Name—Select from the drop-down list the user to whom SNMP notifications are sent. In order to receive notifications, this user must be defined on the SNMP User page, and its engine ID must be remote.
- Security Level—Select how much authentication is applied to the packet.

  NOTE The Security Level here depends on which User Name was selected. If this User Name was configured as No Authentication, the Security Level is No Authentication only. However, if this User Name has assigned Authentication and Privacy on the User page, the security level on this screen can be either No Authentication, or Authentication Only, or Authentication and Privacy.

  The options are:

  - *No Authentication*—Indicates the packet is neither authenticated nor encrypted.
  - *Authentication*—Indicates the packet is authenticated but not encrypted.
  - *Privacy*—Indicates the packet is both authenticated and encrypted.
- **Notification Filter—**Select to enable filtering the type of SNMP notifications sent to the management station. The filters are created in the Notification Filter page.
- **Filter Name—**Select the SNMP filter that defines the information contained in traps (defined in the Notification Filter page).

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

SNMP Notification Filters

The Notification Filter page enables configuring SNMP notification filters and Object IDs (OIDs) that are checked. After creating a notification filter, it is possible to attach it to a notification recipient in the Notification Recipients SNMPv1,2 page, and Notification Recipients SNMPv3 page.

The notification filter enables filtering the type of SNMP notifications that are sent to the management station based on the OID of the notification to be sent.

To define a notification filter:

STEP 1 Click **SNMP** > **Notification Filter**.

The Notification Filter page contains notification information for each filter. The table is able to filter notification entries by Filter Name.

STEP 2 Click **Add**.

STEP 3 Enter the parameters.

- **Filter Name—**Enter a name between 0-30 characters.
- **Object ID Subtree—**Select the node in the MIB tree that is included or excluded in the selected SNMP filter. The options to select the object are as follows:
    - *Select from list*—Enables you to navigate the MIB tree. Press the *Up* arrow to go to the level of the selected node's parent and siblings; press the *Down* arrow to descend to the level of the selected node's children. Click nodes in the view to pass from one node to its sibling. Use the scrollbar to bring siblings in view.
    - If *Object ID* is used, the **entered object identifier** is included in the view if the **Include in filter** option is selected.

STEP 4 Select or deselect **Include in filter.** If this is selected, the selected MIBs are included in the filter, otherwise they are excluded.

STEP 5 Click **Apply**. The SNMP views are defined and the running configuration is updated.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: 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. (1110R)

© 2010-2013 Cisco Systems, Inc. All rights reserved.