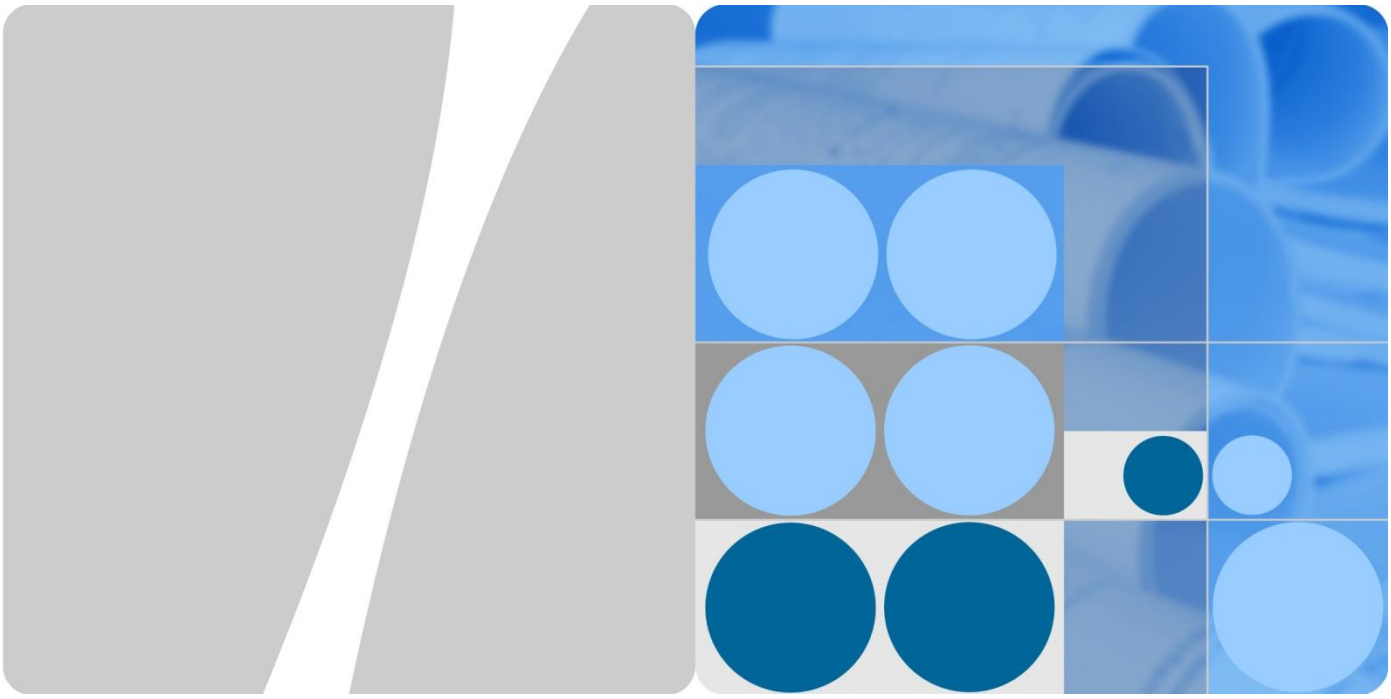


Quidway S1700 Series Switches
V100R006C00

Web User Manual

Issue 02

Date 2012-07-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://enterprise.huawei.com

About This Document

Product Version

The following table lists the product versions associated with this document.

Product Name	Product Version
S1700	V100R006C00

Intended Audience

The Quidway S1700 Series Ethernet Switches (hereinafter referred to as the S1700) used in the Web NMS client.

This paper describes the operational knowledge of the Web NMS client instructions.

This document applies to the following engineers:

- Installation and commissioning engineers
- NM configuration engineers
- Technical support engineers
- FAE
- Network monitoring engineers
- System maintain engineers
- Policy planning engineers

Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
 WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.

Symbol	Description
CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
TIP	Indicates a tip that may help you solve a problem or save time.
NOTE	Provides additional information to emphasize or supplement important points of the main text.

Command Conventions

Format	Description
Boldface	The keywords of a command line are in **Boldface**.
Italic	Command arguments are in <*Italic*.
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x | y | ... } *	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...] *	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.

GUI Conventions

Format	Description
“”	Buttons, menus, parameters, tabs, window, and dialog titles are in boldface. For example, click **OK**.
>	Multi-level menus are in boldface and separated by the ">" signs. For example, choose **File** > **Create Folder**.

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Issue 02 (2012-07-25)

Relative to the version 01(2011-11-17) of the changes are as follows:

1. Updated website.

2. Increase product information page to see.

3. Save the configuration supplementary instructions.

4. VLAN edit / members of the configuration instructions.

5. Corresponding to the traffic prioritization.

6. Update the password configuration requirements.

7. GMP-snooping profile configuration column describes.

Issue 01(2011-11-17)

The first official release.

Contents

1 WEB Configuration

About This Chapter

Use the System menu items to display and configure basic administrative details of the switch.

This section describes the basic switch features, along with a detailed description of how to configure each feature via a web browser.

1.1 Logging In to the Web Interface

Before configuring the switch, you must log in to the web interface.

1.1.1 Background Information

- The Web interface client connects to the switch through HTTP; therefore, you must log in to the Web interface through HTTP.
- The Web interface supports the Microsoft Internet Explorer 6.0 (IE6.0) or above, Mozilla Firefox 4.0 or above, and Chrome. The Web interface described in this document uses the IE8.0.

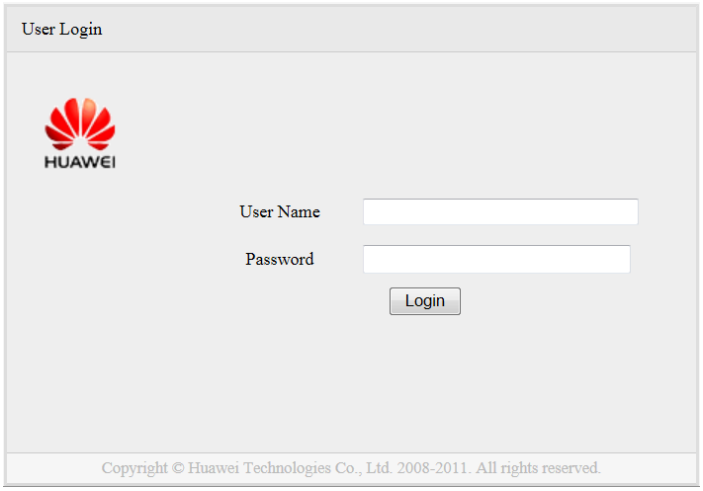
1.1.2 Connecting to the Web Interface

Prior to accessing the switch from a web browser, be sure you have first performed the following tasks:

1. Open IE browser .
2. Enter the default IP address: http://192.168.0.1. Press ENTER.

   The user login dialog box is displayed, see Figure 1-1.

Figure 1-1 User Login



3. Enter values in User Name and Password. Click LOGIN.
   - The default User Name and Password of S1700 are admin， Admin@123
   - Users can modify the password, change your password the detailed requirements please refer to the "Safety> User Accounts> Modify" the description in the chapter.
4. The system configuration program is displayed after logging in to the Web interface.

----End

NOTE

1. Super user user name admin password, can't delete, configurable.

2. The user to reconfigure the password, follow the password complexity requirements configuration.

3. View product information users to log in to access, hidden page access URL is: http://192.168.0.1/help/mfg_info.htm

1.2 Navigating the web browser interface

The following sections help you understand the Web interface and improve your operation efficiency.

1.2.1 Home page

The layout and style of the Web interface are described in this section.

Figure 1-2 shows a typical operation user interface of the Web interface.

Figure 1-2 Home page

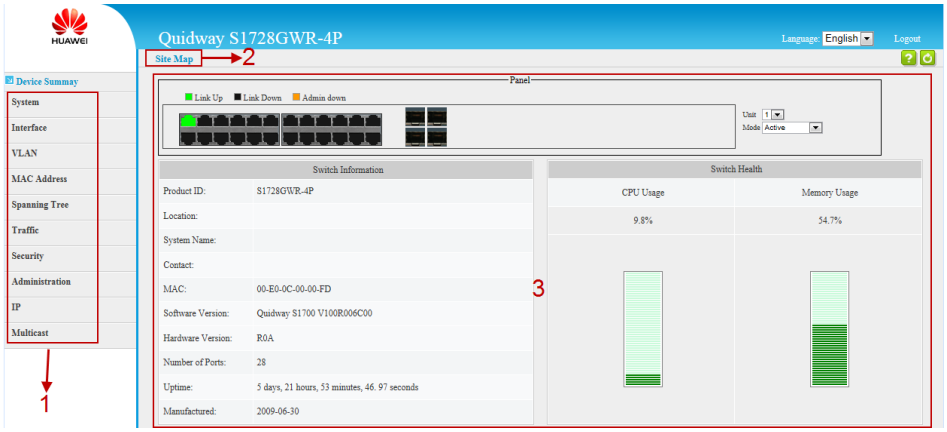


Table 1-1 Home page

Title	Description
1	Main Menu
2	Your location
3	System Information

1.2.2 Navigation Tree

The navigation tree consists of ten nodes: System, Interface, VLAN, MAC Address, Spanning Tree, Traffic, Security, Administration, IP, and Multicast.

Table 1-2 Switch Main Menu

Menu	Sub-Menu	Description
System	General	Provides basic system description, system uptime, system name, system location, system contact, system jumbo frame and system EEE.
	IP	Displays and Sets VLAN and the IPv4 address for management access and displays local MAC address, etc.
	File	• Upgrade: upgrade the firmware for switch. • Set start-up：Sets the startup file • Show/Delete：Shows the files stored in flash memory; allows deletion of files. • Config file: Save/Upload/Download the config file of the switch.
	Time	Manually setts the current time.
	CPU Utilization	Displays information on CPU utilization

Menu	Sub-Menu	Description
	Memory Usage	Shows memory utilization parameters
	Reset	Restarts the switch immediately.
	RFID	QA information by Huawei factory, to confirm if the factory device system is normal and to guarantee every device has the right version.
Interface	Port	• General: Configures connection settings per port, Configures connection settings for a range of ports, Displays port connection status. • Mirror: Sets the source and target ports for mirroring, Shows the configured mirror sessions, • Statistics: Show Interface statistics. • Cable Test: Performs cable diagnostics for selected port to diagnose any cable faults (short, open etc.) and report the cable length
	Trunk	• System Priority: Configuring system priority • Static: Configuring Static/Manul Trunks • Statistics: Show statistics of trunk.
	Transceiver	Information: show information of transceiver.
	Green Ethernet	Enable or disable the power saving mode on the specified port.
VLAN	Static	Configures Static VLAN: Add, Show/Delete, Modify, Edit/Show Member by VLAN, Edit/Show Member by interface, and Edit member by Interface Range.
MAC Address	Static	Configures Static MAC Addresses: Add, Show/Delete.
	Dynamic	Configures Dynamic MAC Addresses: Show Dynamic MAC, Clear Dynamic MAC, and Configure Aging.
Spanning Tree	STP	Configures STP parameters: Configure Global, Configure Interface.
Traffic	Rate Limit	Sets the output rate limits for a port
	Storm Cotrol	Configuring strom control.
	Priority	Sets the default priority for each port or trunk, Queue, Trust mode,DSCP to DSCP, CoS to DSCP PHB to Queue
	Voice VLAN	Configuring Voice VLAN.
Security	AAA	Sets system authentication, server
	User Accounts	Configuring user accounts.
	Network Acceess	Configuring network access.
	IP Filter	Configuring IP filtering.

Menu	Sub-Menu	Description
	Port Isolation	Configuring port isolation.
	Port Authentication	Configuring port authentication.
Administration	Log	Configuring system, remote log of administrator
	LLDP	Configuring LLDP
IP	General	Configuring Ping
	ARP	Configuring ARP
Multicast	IGMP Snoopoing	Configuring IGMP related parameters, such as general, multicast router, IGMP member, Interface, forwarding entry

1.2.3 Buttons

The buttons that you usually use on the Web interface are described in this section.

Table 1-3 describes the buttons and functions.

Table 1-3 Button description

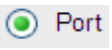
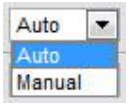
Button	Action
Apply	Sets specified values to the system.
Revert	Cancels specified values and restores current values prior to pressing "Apply."
Test	Click to test the corresponding testing.
Delete	Click to delete the selected data.
Reset	Click to reset the swtich.
Clear	Click to clear the statistics on the system.
Refresh	Click to refresh the statistics on the system.
Default	Click to reset the configuration settings to the factory defaults.
Query	Click to query on the system.

1.2.4 Common Interface Elements

The elements that you usually use on the Web interface are described in this section.

Table 1-4 describes the common elements that you usually use on the Web interface.

Table 1-4 Common Interface Elements

Element	Description
Button	
Page selection button	
Radio button	
Check Box	
Text box	
Drop-down list	
Help	
refresh	

1.3 Idle-Time

If you do not perform any operation on the web interface for a long time, you are logged out and the longin page is displayed. If you need to continue operations, log in again.

Figure 1-1 shows the login page.

NOTE
Default idle time is 20minites.

1.4 Save Configuration

After performing configuration, you need to save the configuration data.

CAUTION
If you do not save the configuration data, the configuration that you made will be lost after modifying or refreashing.

1.5 Logout

After the configuration finished, sugguest to logout to ensure the system security.

Following is the 2ways to logout.

- Click the  button to close the web browser.
- Click the  to logout the system.

2 Site Map

About This Chapter

This chapter describes the following topics: Panel Display, Switch Information, and swtich health.

2.1 Panel Display

This section provides information about the device panel.

Click **Device Summary** in the navigation tree to open the **Device Summary** page. You can view the panel tab page, as shown in Figure 2-1.

Figure 2-1 Front panel Indicators

The panel area on the Web interface displays information about each port of the selected switch, including:

- Number of ports
- Operating mode of each port: Active, Duplex, and Flow Control.

NOTE

You can place the cursor on a port to view the port number.

2.2 Displaying Switch Information

This section displays the product ID, Location, System Name, Contact, MAC, Software Version, number of Ports, Uptime, and manufactured.

Click **Device Summary** in the navigation tree to open the **Device Summary** page. You can view the **Switch Information** page, as shown in Figure 2-2.

Figure 2-2 Switch Information

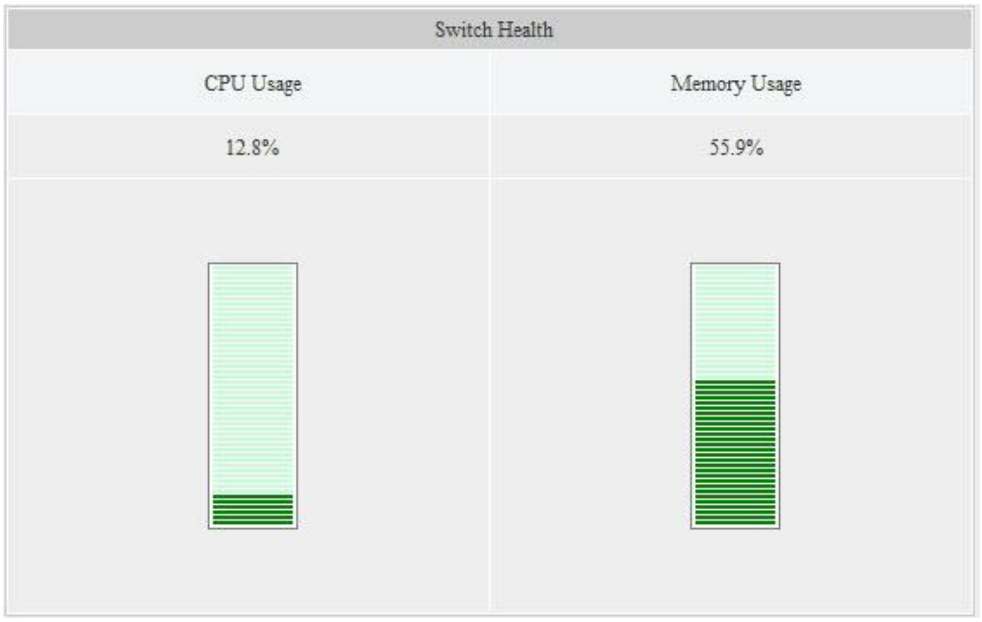
Switch Information	
Product ID:	S1728GWR-4P
Location:	
System Name:	
Contact:	
MAC:	00-E0-0C-00-00-FD
Software Version:	Quidway S1700 V100R006C00
Hardware Version:	R0A
Number of Ports:	28
Uptime:	5 days, 21 hours, 53 minutes, 46. 97 seconds
Manufactured:	2009-06-30

2.3 Switch Health

This section displays the current CPU usage and Memory Usage.

Click **Device Summary** in the navigation tree to open the **Device Summary** page. You can view the **Switch Heath** page, as shown in Figure 2-3.

Figure 2-3 Switch Health



3 System Management

About This Chapter

This chapter describes the following topics:

3.1 Setting System General Information

Use the System > General page to identify the system by the information displayed, including the System Information, System UP Time, System Name, System Location, System Contact, System Jumbo Frame, and System EEE, as shown in Figure 3-1.

Figure 3-1 "System > General" Information

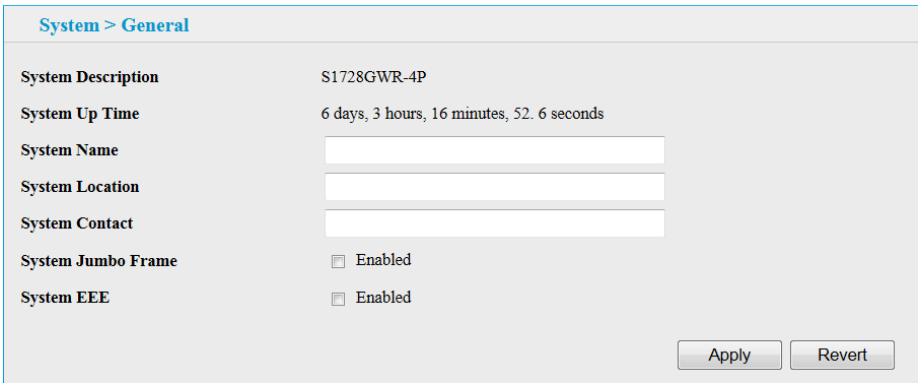


Table 3-1 Parameters of "System > General" Information

Title	Description
System Description	Brief description of device type
System Up Time	Length of time the management agent has been up.
System Name	Name assigned to the switch system
System Location	Specifies the system location.
System Contact	The contact information of the administrator
System Jumbo Frame	Enable or disable system jumbo frame. (default:disabled)
System EEE	Enable or disable system EEE. (default:disabled)

1. Click System > General.
2. Specify the system name, location, and contact information for the system administrator, enable or disable system jumbo frame and system EEE.
3. Click Apply.

----End

3.2 Setting the Switch's IP Address

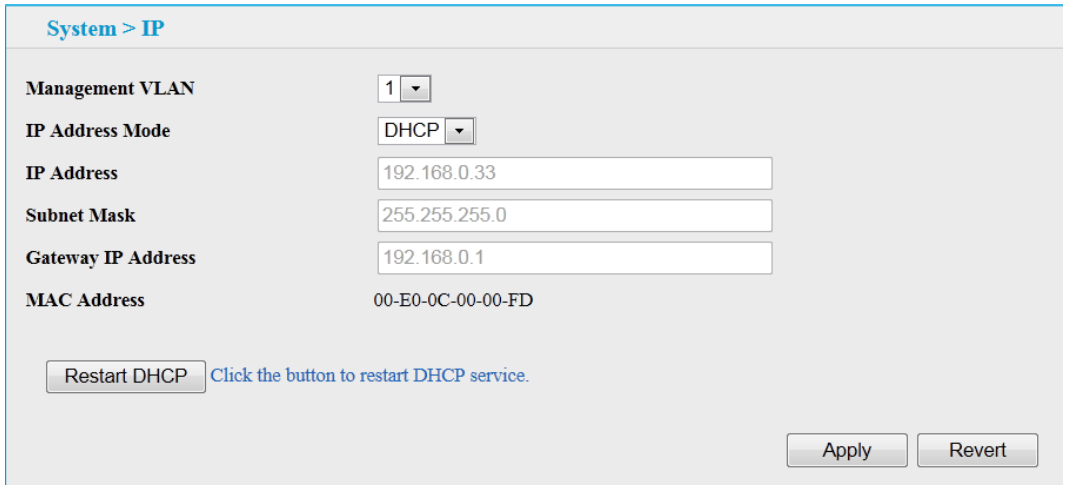
Use the System > IP page to configure VLAN and an IPv4 address for management access over the network.

At default, the device obtains an address from DHCP server. If failed to obtain IP address, a static address of 192.168.0.1 will be assigned.

To obtain a dynamic address through DHCP for the switch:

1. Click System > IP.
2. Select the VLAN through which the management station is attached, set the IP Address Mode to "DHCP".
3. Click Apply to save your changes.
4. Then click Restart DHCP to immediately request a new address.

Figure 3-2 Configuring a DHCP IPv4 Address



----End

To set a static address for the switch:

1. Click System > IP.
2. Select the VLAN through which the management station is attached, set the IP Address Mode to “Static,” enter the IP address, subnet mask and gateway.
3. Click Apply.

Figure 3-3 Configuring a Static IPv4 Address

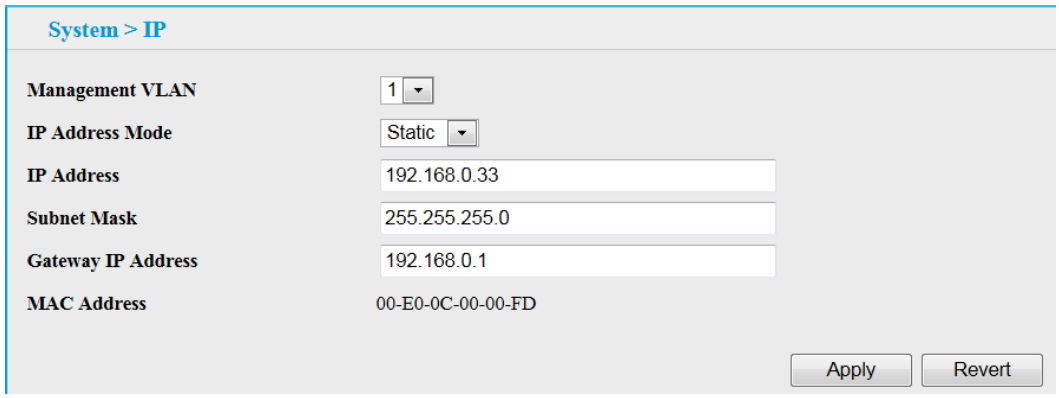


Table 3-2 Parameter of Configuring IP Address for Switch

Title	Description
Management VLAN	ID of the configured VLAN (1-4093). By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.

Title	Description
IP Address Mode	Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP). If DHCP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. DHCP responses can include the IP address, subnet mask, and default gateway. (Default: DHCP)
IP Address	Address of the VLAN to which the management station is attached. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 192.168.0.1)
Subnet Mask	This mask identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)
Gateway IP Address	IP address of the gateway router between the switch and management stations that exist on other network segments. (Default: null)
MAC Address	Show the Physical address for this switch.
Restart DHCP	Click to restart DHCP service.

----End

3.3 Managing System Files

Use the System > File page to manage the switch system files, including upgrading the switch operating software or configuration files, setting the system start-up files, etc.

3.3.1 Upgrade Firmware

Use the System > File (Upgrade) page to upgrade the firmware to use for system initialization.

To upgrade the firmware for switch:

1. Click System > File, see Figure 3-4.
2. Select Upgrade from the Action list.
3. Set the corresponding configuration parameters, and then click Apply.
   SeeTable 3-3 for the parameters of upgrade switch.

Figure 3-4 Upgrade Switch

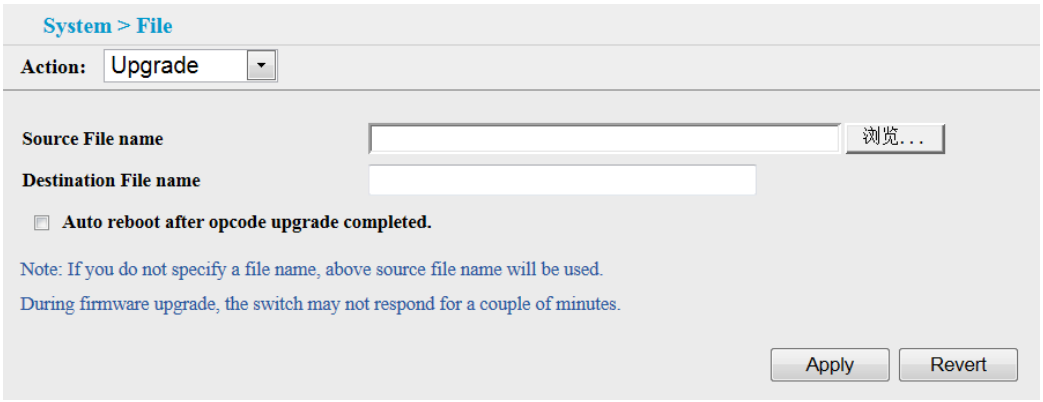


Table 3-3 Parameter of Upgrade Switch

Title	Description
Action	Select upgrade to upgrade the firmware (Required).
Source File name	The file name of the firmware in the management station. Click"Browse"button to choose the upgrading firmware. For example: S1700_V100R006C00B003.bin.
Destination File name	The destination file name of the firmware in the switch. The file name should not contain slashes(or /), the leading letter of the file name should not be a period (.), and the maximum, length for file names is 63 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_").
Auto reboot after opcode upgrade completed	Enable the check box to auto reboot after opcode upgrade completed.

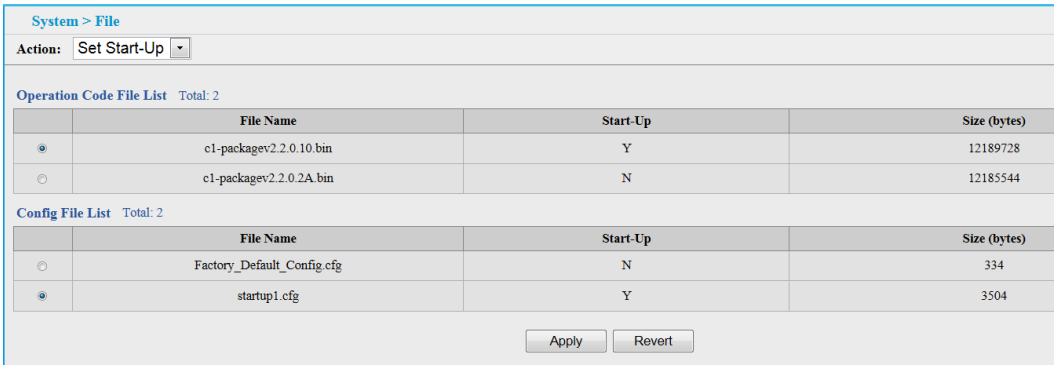
4. The switch reboot automatically if you enable the chck box Auto reboot after opcode upgrade completed. After rebooting, the page automatically jumps to the login page when you click it.
5. Input User Name and Password to log in the Web interface.

----End

3.3.2 Setting the Start-Up File

Use the System > File (Set Start-Up) page to specify the firmware or configuration file to use for system initialization.

Figure 3-5 Setting Start-Up Files



1. Click System > File. See Figure 3-5.
2. Select Set Start-Up from the Action list.
3. Mark the operation code or configuration file to be used at startup.Click Apply, and it takes effect when you reboot the system.

Table 3-4 Parameter of Upgrade Switch

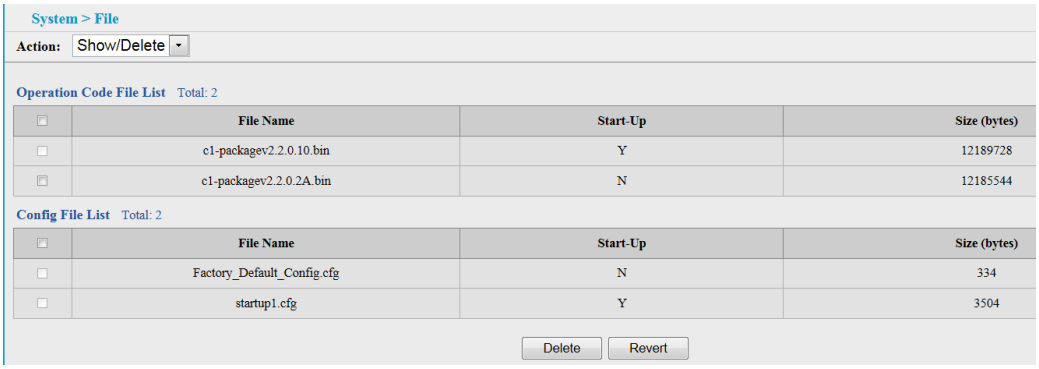
Title	Description
Action	Select Set Start-Up to specify the Start-Up file (Required).
File name	The Start-Up File. Mark the Operation Code File List and Config File List (Required).
Start-Up	Activation status. “Y”means the corresding file is the Start-Up file. “N”means not.
Size (bytes)	The size of this file.

----End

3.3.3 Showing/Deleting System Files

Use the System > File (Show/Delete) page to show the files in the system directory, or to delete a file.

Figure 3-6 Showing System Files



1. Click System, then File.
2. Select Show from the Action list.
3. To delete a file, mark it in the File List and click Delete.

Table 3-5 Parameter of Upgrade Switch

Title	Description
Action	Select Show/Delete to Show/Delete the switch system file (Required).
File name	The Start-Up File.
Start-Up	Activation status. “Y”means the corresding file is the Start-Up file. “N”means not.
Size (bytes)	The size of this file.

CAUTION

Files designated for start-up, and the Factory_Default_Config.cfg file, cannot be deleted.

----End

3.3.4 Saving the Running Configuration to a Local File

Use the System > File (Config File) page to save the current configuration settings to a local file and to upload/download configuration files by using HTTP. See Figure 3-7, Figure 3-8, and Figure 3-9.

Figure 3-7 Saving the Running Configuration

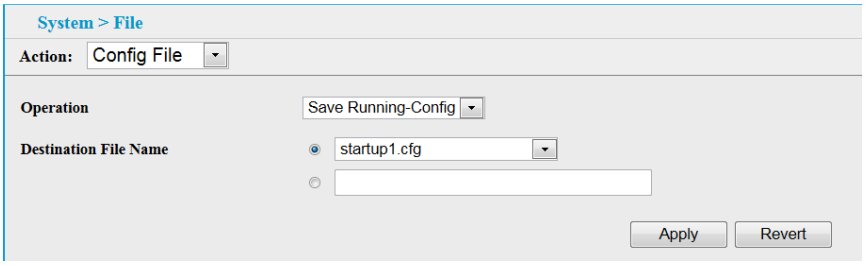


Figure 3-8 HTTP Uploading Configuration

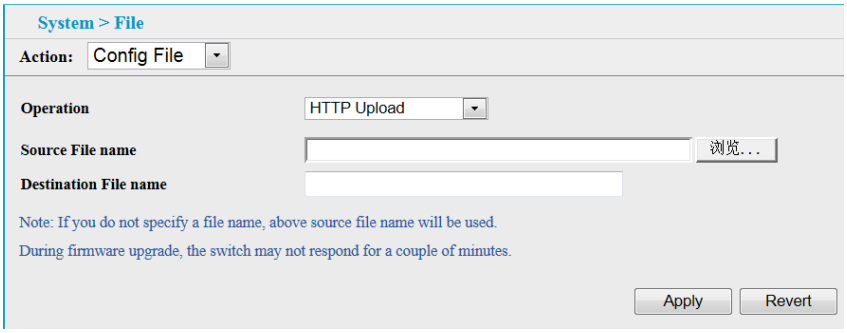
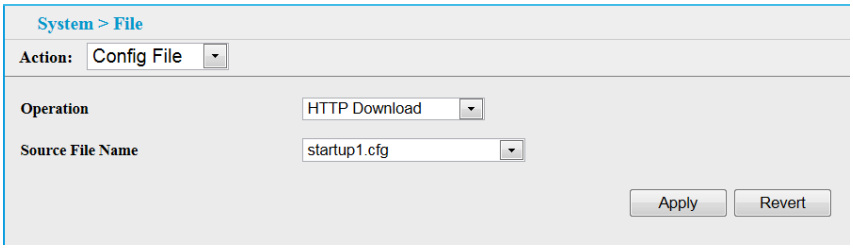


Figure 3-9 HTTP Downloading Configuration



1. Click System > File. Figure 3-7 is displayed.
2. Select Config File from the Action list.
3. Select "save the current configuration" from the operation list.
4. Choose needs to be saved in the Save as file name, or rename files.
5. Click Apply, save the current configuration.

To upload / download configuration file, as shown in Figure 3-8 or 3-9, need to upload / download the source file, click the "Apply" operation, Table 3-6 describes the operation parameters.

Table 3-6 Operation Parameters

Title	Description
Save Running-Config	Copies the current configuration settings to a local file on the switch.
HTTP Upload	Uploads the PC local configuration files to the switch system by using HTTP. Specify Destination file names.
HTTP Download	Downloads the original configuration files to the local PC.

----End

3.4 Setting the System Clock

Use the System > Time page to set the system time on the switch manually.

Figure 3-10 Manually Setting the System Clock

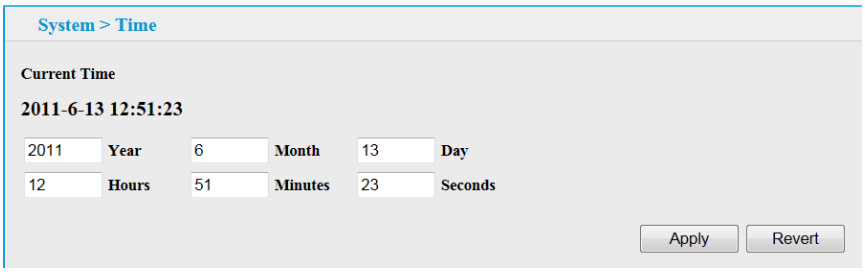


Table 3-7 Manually Setting the System Clock Parameters

Title	Description
Current Time	Shows the current time set on the switch.
Year	Sets the year. (Range: 1970-2037)
Month	Sets the month. (Range: 1-12)
Day	Sets the day of the month. (Range: 1-31)
Hours	Sets the hour. (Range: 0-23)
Minutes	Sets the minute value. (Range: 0-59)
Seconds	Sets the second value. (Range: 0-59

1. Click System > Time.
2. Enter the time and date in the appropriate fields as required.

3. Click Apply.

----End

3.5 Displaying CPU Utilization

Use the System > CPU Utilization page to display information on CPU utilization.

Figure 3-11 Displaying CPU Utilization

Table 3-8 Displaying CPU Utilization Parameters

Title	Description
Time Interval	The interval at which to update the displayed utilization rate. (Options: 1, 5, 10, 30, 60 seconds; Default: 1 second)
CPU Utilization	CPU utilization over specified interval in percentage.

To display CPU utilization:

1. Click System > CPU Utilization.
2. Change the update interval if required. Note that the interval is changed as soon as a new setting is selected.

----End

3.6 Displaying Memory Usage

Use the System > Memory Usage page to display memory usage parameters.

Figure 3-12 Displaying Memory Usage

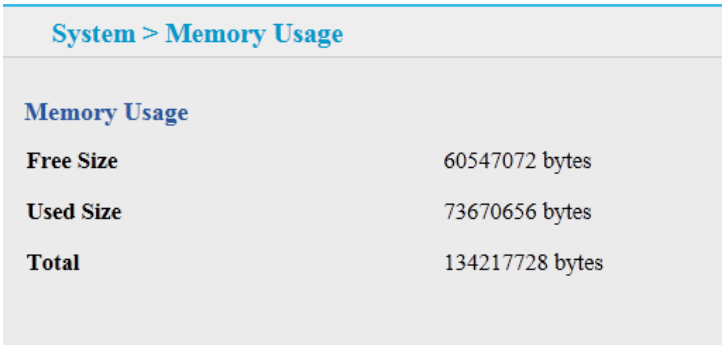


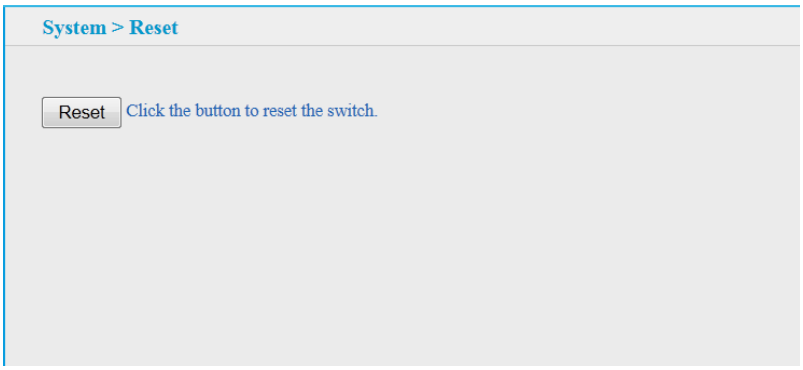
Table 3-9 Displaying Memory Usage Parameters

Title	Description
Free Size	The amount of memory currently free for use.
Used Size	The amount of memory allocated to active processes.
Total	The total amount of system memory.

3.7 Resetting the System

Use the System > Reset menu to restart the switch.

Figure 3-13 Restarting the Switch



3.8 Displaying RFID

Use the System > RFID menu to show RFID information.

Figure 3-14 RFID

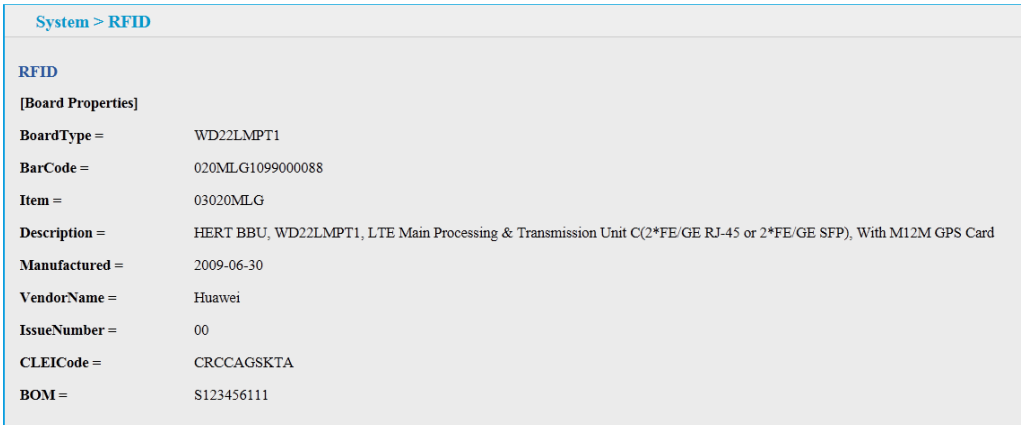


Table 3-10 Displaying RFID Information

Title	Description	Source	Format
Board Type	Type of FRU (Board, Back Panel, Power, etc). T with the exsiting standards, English title for short is still Board Type.	Be consistent with the information displayed in Attribute > Internal Type in PDM	String E.g: SSA1SL1601 (Take optical network products as example, the same below)
BarCode	FRU BarCode	The attached bar code for board: finished board or manufactured board; the configuration board bar code: the top level bar code for boards or parts	String E.g: 0359231049000004
Item	BBOM Code	Be consistent with the information displayed in Code for parts in PDM; for board, the BBOM Code is for produced board.	String E.g:03032760
Description	The description of FRU	Be consistent with the information displayed in English Description for parts in PDM	String E.g:OptiX 10G(V2.0),SSA1SL1601,STM-16 Optical Interface Board(S-16.1,SC)
Manufactured	The date of MRU manufactured	The date that RFU is stored into the tag	YYYY-MM-DD E.g:2002-01-23

Title	Description	Source	Format
VendorName	The name of Vendor Name	The vendor name is “Huawei” for the products produced in huawei or the products outsourced to other companies. The vendor name is the corresponding supplier name for the products purchased by Huawei.	String E.g：Huawei
Issue number	Issue number	The sub-version of hardware and the data is from the supply chain of IT system.	String Numbers only. E.g：00
CLEI Code	The CLEI Code of FRU	The international standard material code	String Captitals and numbers only E.g：FC9612PW11
BOM	Precise item code of FRU	More precise item code only reserved for the products that Huawei Item can not meet the customer asset management.	String Captitals and numbers only E.g： BOM030702250119360

4 Interface Configuration

About This Chapter

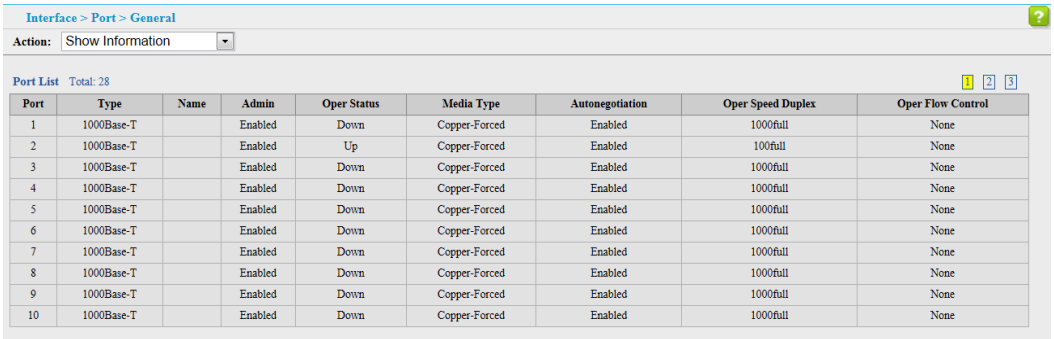
4.1 Port Configuration

This section describes how to configure port connections, mirror traffic from one port to another, and run cable diagnostics.

4.1.1 General

Use the Interface > Port > General (Show Information) page to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

Figure 4-1 Displaying Port Information



Port	Type	Name	Admin	Oper Status	Media Type	Autonegotiation	Oper Speed Duplex	Oper Flow Control
1	1000Base-T		Enabled	Down	Copper-Forced	Enabled	1000full	None
2	1000Base-T		Enabled	Up	Copper-Forced	Enabled	100full	None
3	1000Base-T		Enabled	Down	Copper-Forced	Enabled	1000full	None
4	1000Base-T		Enabled	Down	Copper-Forced	Enabled	1000full	None
5	1000Base-T		Enabled	Down	Copper-Forced	Enabled	1000full	None
6	1000Base-T		Enabled	Down	Copper-Forced	Enabled	1000full	None
7	1000Base-T		Enabled	Down	Copper-Forced	Enabled	1000full	None
8	1000Base-T		Enabled	Down	Copper-Forced	Enabled	1000full	None
9	1000Base-T		Enabled	Down	Copper-Forced	Enabled	1000full	None
10	1000Base-T		Enabled	Down	Copper-Forced	Enabled	1000full	None

Table 4-1 Parameters of Displaying Port Information

Title	Description
Port	Port identifier.
Type	Indicates the port type. (1000Base-T, 1000Base SFP)
Name	Interface label.
Admin	Shows if the port is enabled or disabled.
Oper Status	Indicates if the link is Up or Down.
Media Type	Media type used. (Options: RJ-45 – Copper-Forced; SFP-Forced,; Default: RJ-45 – Copper-Forced)
Autonegotiation	Shows if auto-negotiation is enabled or disabled.
Oper Speed Duplex	Shows the current speed and duplex mode.
Oper Flow Control	Shows if flow control is enabled or disabled.

To display port connection parameters:

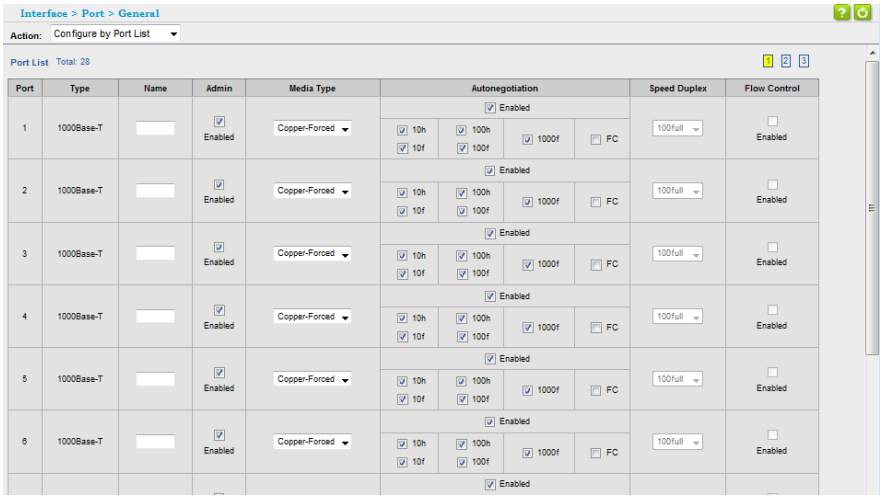
1. Click Interface > Port > General. Figure 4-1 is displayed.
2. Select Show Information from the Action List.

----End

Configuring by Port List

Use the Interface > Port > General (Configure by Port List) page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

Figure 4-2 Configuring Connections by Port List



- Auto-negotiation must be disabled before you can configure or force an interface to use the Speed/Duplex mode or Flow Control options.
- When using auto-negotiation, the optimal settings will be negotiated between the link partners based on their advertised capabilities. To set the speed, duplex mode, or flow control under auto-negotiation, the required operation modes must be specified in the capabilities list for an interface.
- The 1000BASE-T standard does not support forced mode. Autonegotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.
- The Speed/Duplex mode is fixed at 1000full on the Gigabit SFP ports. When auto-negotiation is enabled, the only attributes which can be advertised include flow control.

Table 4-2 Parameters of Configuring Connections by Port List

Title	Description
Port	Port identifier.
Type	Indicates the port type. (1000Base-T, 1000Base SFP)
Name	Allows you to label an interface. (Range: 1-64 characters)
Admin	Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable an interface for security reasons.
Media Type	• Copper-Forced:Always uses the built-in RJ-45 port. • SFP-Forced: ways uses the SFP port (even if a module is not installed).
Autonegotiation	Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow control.The following capabilities are supported.
Speed/Duplex	Allows you to manually set the port speed and duplex mode. (i.e., with auto-negotiation disabled)
Flow Control	Allows automatic or manual selection of flow control.

1. Click Interface > Port > General. Select Configure by Port List from the Action List.

   Figure 4-2 is displayed.

2. Modify the required interface settings. Go to next page by clocking  .
3. Click Apply. It takes effect immediately.

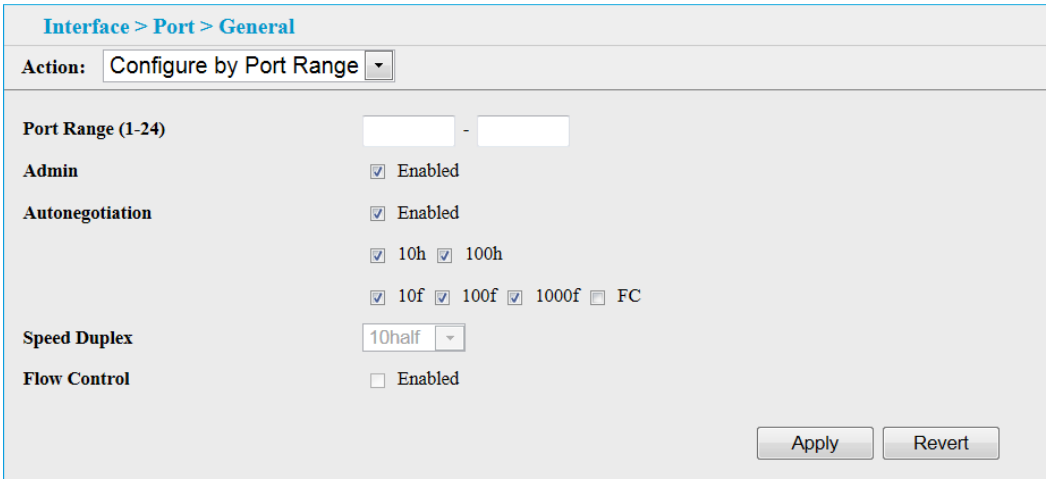
   View the port status by clicking Interface > Port > General and selecting Show Information from the Action List.

   ----End

Configuring by Port Range

Use the Interface > Port > General (Configure by Port Range) page to enable/disable interfaces, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

Figure 4-3 Configuring Connections by Port Range



1. Click Interface > Port > General. Select Configure by Port Range from the Action List.

   Figure 4-3 is displayed.

2. Specify the Port Range and setup the configuration parameters.

3. Click Apply. It takes effect immediately.

   View the port status by clicking Interface > Port > General and selecting Show Information from the Action List.

   ----End

4.1.2 Configuring Local Port Mirroring

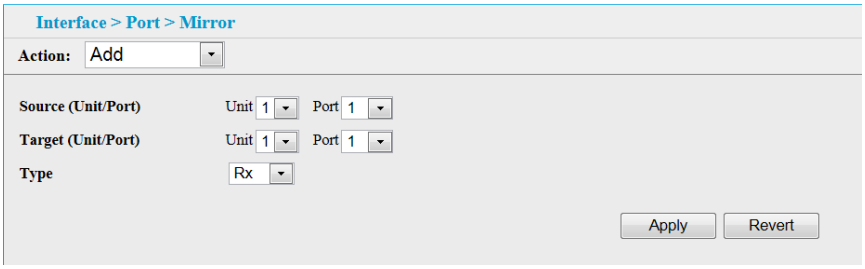
Use the Interface > Port > Mirror page to mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

- Traffic can be mirrored from one or more source ports to a destination port on the same switch (local port mirroring as described in this section).
- Target port speed should match or exceed source port speed, otherwise traffic may be dropped from the target port.

To add a local mirror session:

1. Click Interface > Port > Mirror. Select Add from the Action List. Figure 4-4 is displayed.

Figure 4-4 Configuring Local Port Mirroring



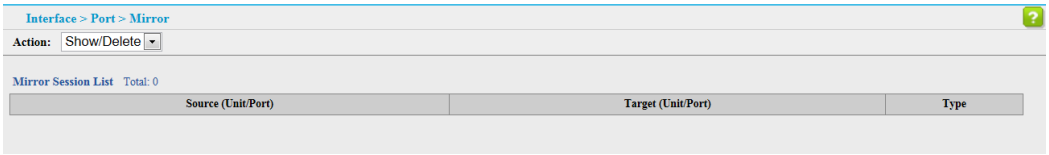
2. Specify the source port, the target port, and the traffic type to be mirrored. See Table 4-3.

Table 4-3 Parameters of Configuring Local Port Mirroring

Title	Description
Source Port	The port whose traffic will be monitored. The value range of port number is 1~28.
Target Port	The port that will mirror the traffic on the source port. The value range of port number is 1~28.
Type	Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both. (Default: Rx)

3. Click Apply. Select Show/Delete from the Action List to dsplay the local port mirror sessions. See Figure 4-5.

Figure 4-5 Displaying Local Port Mirror Sessions



----End

4.1.3 Showing Port Statistics

Use the Interface > Port > Statistics page to display standard statistics on network traffic from the Interface. All values displayed have been accumulated since the last system reboot, and are shown as counts per second.

To show a list of port statistics:

1. Click Interface > Port > Statistics.
2. Select a port from the drop-down list. See Figure 4-6.
3. Use the Refresh button at the bottom of the page if you need to update the screen.

Figure 4-6 Showing Port Statistics

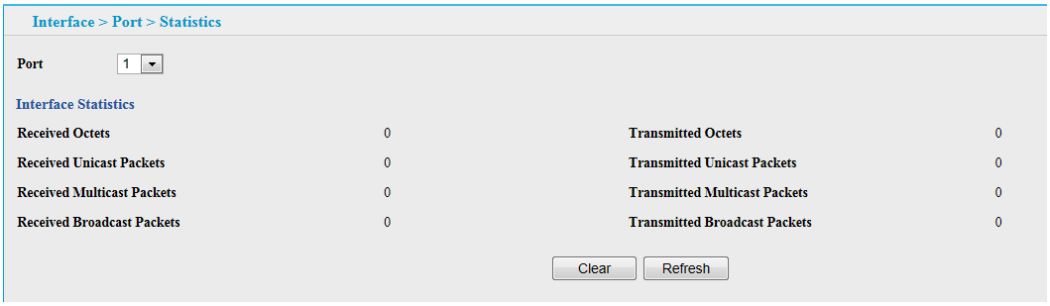


Table 4-4 Parameters of Port Statistics-Interface

Title	Description
Received Octets	The total number of octets received on the interface, including framing characters.
Transmitted Octets	The total number of octets transmitted out of the interface, including framing characters.
Received Unicast Packets	The total number of received unicast packets.
Transmitted Unicast Packets	The total number of transmitted unicast packets.
Received Multicast Packets	The total number of received multicast packets.
Transmitted Multicast Packets	The total number of transmitted multicast packets.
Received Broadcast Packets	The total number of received broadcast packets.
Transmitted Broadcast Packets	The total number of transmitted broadcast packets.

----End

4.1.4 Performing Cable Diagnostics

Use the Interface > Port > Cable Test page to test the cable attached to a port. The cable test will check for any cable faults (short, open, etc.). If a fault is found, the switch reports the length to the fault. Otherwise, it reports the cable length. It can be used to determine the quality of the cable, connectors, and terminations. Problems such as opens, shorts, and cable impedance mismatch can be diagnosed with this test.

- Cable diagnostics are performed using Time Domain Reflectometry (TDR) test methods. TDR analyses the cable by sending a pulsed signal into the cable, and then examining the reflection of that pulse.
- This cable test is only accurate for cables 20- 140 meters long.
- The test takes approximately 10 seconds. The switch displays the results of the test immediately upon completion, including common cable failures, as well as the status and approximate length to a fault.

To test the cable attached to a port:

1. Click Interface > Port > Cable Test.

Figure 4-7 Performing Cable Tests

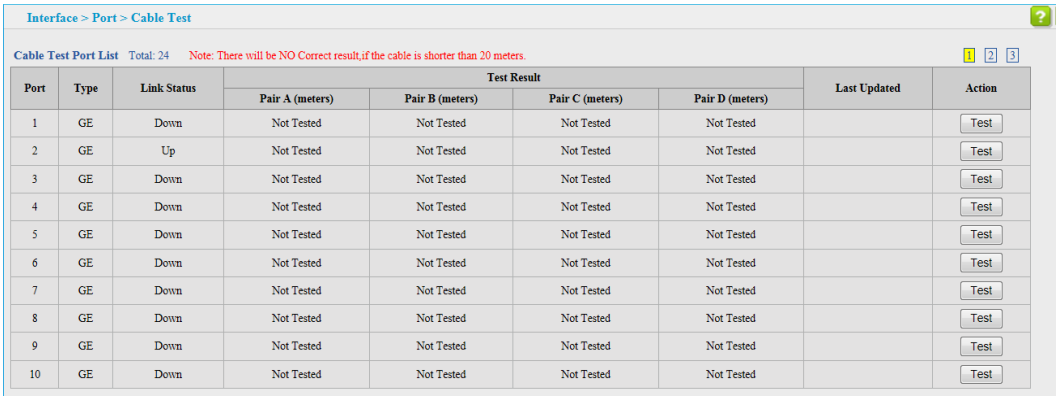


Table 4-5 Parameters of Cable Tests

Title	Description
Port	Switch port identifier.
Type	Displays interface type. (FE – Fast Ethernet, GE – Gigabit Ethernet)
Link Status	Shows if the port link is up or down.
Test Result	The results include common cable failures, as well as the status and approximate distance to a fault, or the approximate cable length if no fault is found.
Last Updated	Shows the last time this port was tested.

2. Click Test for any port to start the cable test. Website will refresh and show the testing result after about 10secends.

----End

4.2 Trunk Configuration

This section describes how to configure static and dynamic trunks.

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a faulttolerant link between two devices. You can create up to 12 trunks at a time on the switch.

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than eight ports, all other ports will be placed in standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

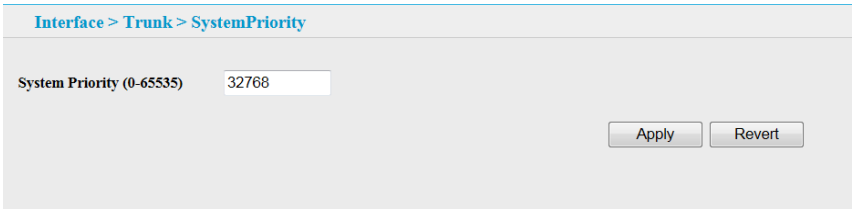
Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the web interface or CLI to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create up to 12 trunks on a switch, with up to eight ports per trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

4.2.1 Configuring System Priority

Use the Interface > Trunk > System Priority page to config system priority of Static Trunk.

Figure 4-8 Configure System Priority



4.2.2 Configuring a Trunk

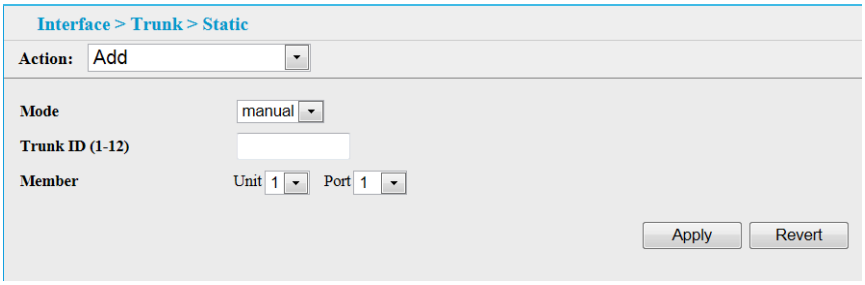
Use the Interface > Trunk > Static page to create a trunk, assign member ports, and configure the connection parameters.

- When configuring trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation. However, note that the static trunks on this switch are Cisco EtherChannel compatible.
- To avoid creating a loop in the network, be sure you add a trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.

To create a static trunk:

1. Click Interface > Trunk > Static. Figure 4-9 is displayed.

Figure 4-9 Creat a Trunk



2. Select Add from the Action list. Enter a trunk identifier, and mark the ports assigned to each trunk. See Table 4-6 for the description of parameters of creating a trunk.

Table 4-6 Parameters of Creating a Trunk

Title	Description
Mode	Manual mode(Manually port aggregation) or static mode (Static LACP port aggregation), 12 groups of up to 8 ports.
Trunk ID	Trunk identifier. (Range: 1-12)
Trunk Member Port List	The ports assigned to a trunk.

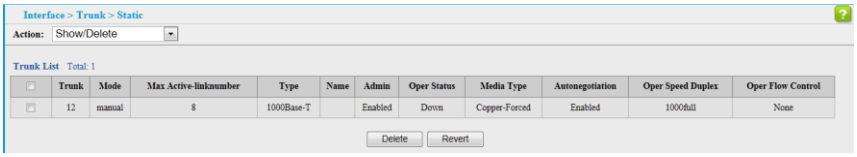
3. Click Apply.

----End

To show/delete the trunks configured on the switch:

1. Click Interface > Trunk > Static.
2. Select Show/Delete from the Action list. Figure 4-10 is displayed.

Figure 4-10 Showing/Deleting Information for Trunks

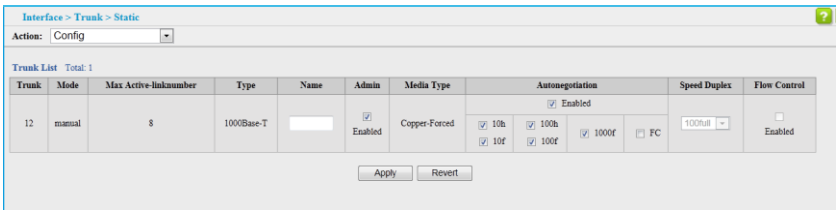


----End

To configure connection parameters for a trunk:

1. Click Interface > Trunk > Static. Select Config from the Action list. Figure 4-11 is displayed.
2. Modify the required interface settings.
3. Click Apply.

Figure 4-11 Configuring Connection Parameters for a Trunk

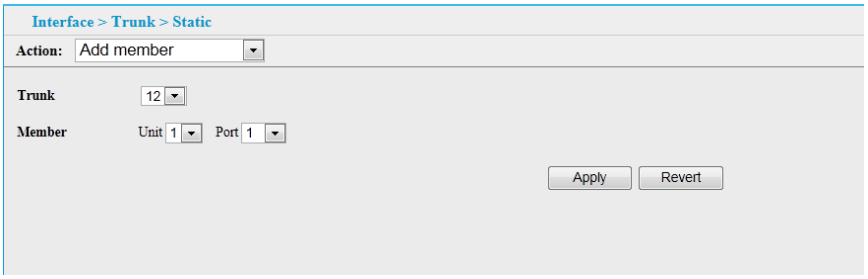


----End

To add member for a trunk configured on the switch:

1. Click Interface > Trunk > Static. Select Add member from the Action list. Figure 4-12 is displayed.
2. Select a trunk identifier, and mark the ports assigned to the trunk.
3. Click Apply.

Figure 4-12 Adding member for Trunks

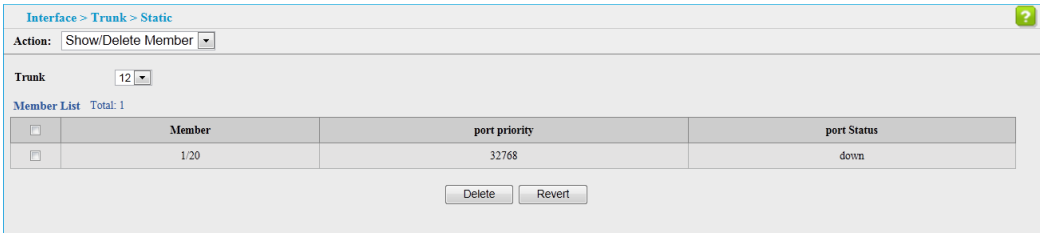


----End

To show/delete the member of the trunk:

1. Click Interface > Trunk > Static. Select Show/Delete Member from the Action list. Figure 4-13 is displayed.

Figure 4-13 Showing/Deleting Member of the Trunk



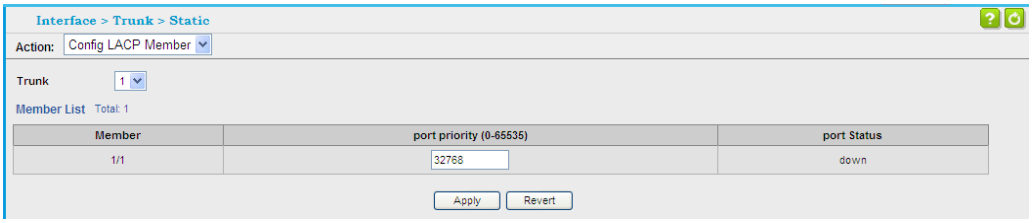
2. Click Delete.

----End

To Config LACP Member of the trunk:

1. Click Interface > Trunk > Static. Select Config LACP Member from the Action list. Figure 4-14 is displayed.

Figure 4-14 Config LACP Member of the Static Trunk



2. Set the trunk member and the priority.

----End

4.2.3 Showing Trunk Statistics

Use the Interface > Trunk > Statistics page to display standard statistics on network traffic from the trunk. Trunk statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). All values displayed have been accumulated since the last system reboot, and are shown as counts per second.

To show a list of trunk statistics:

1. Click Interface > Trunk > Statistics.
2. Select a trunk from the drop-down list. Figure 4-15 is displayed.
3. Use the Refresh button at the bottom of the page if you need to update the screen.

Figure 4-15 Showing Trunk Statistics

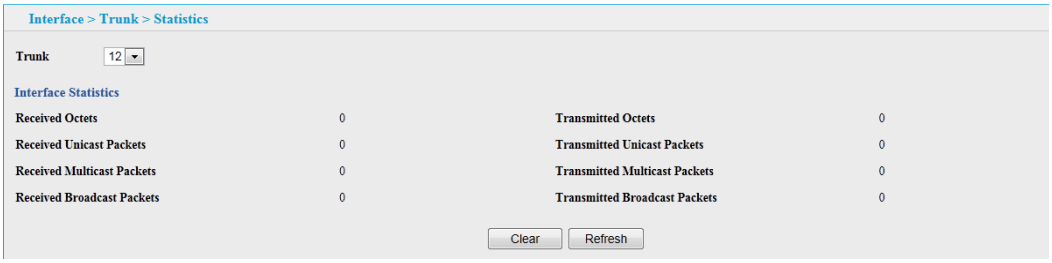


Table 4-7 Parameters of Trunk Statistics

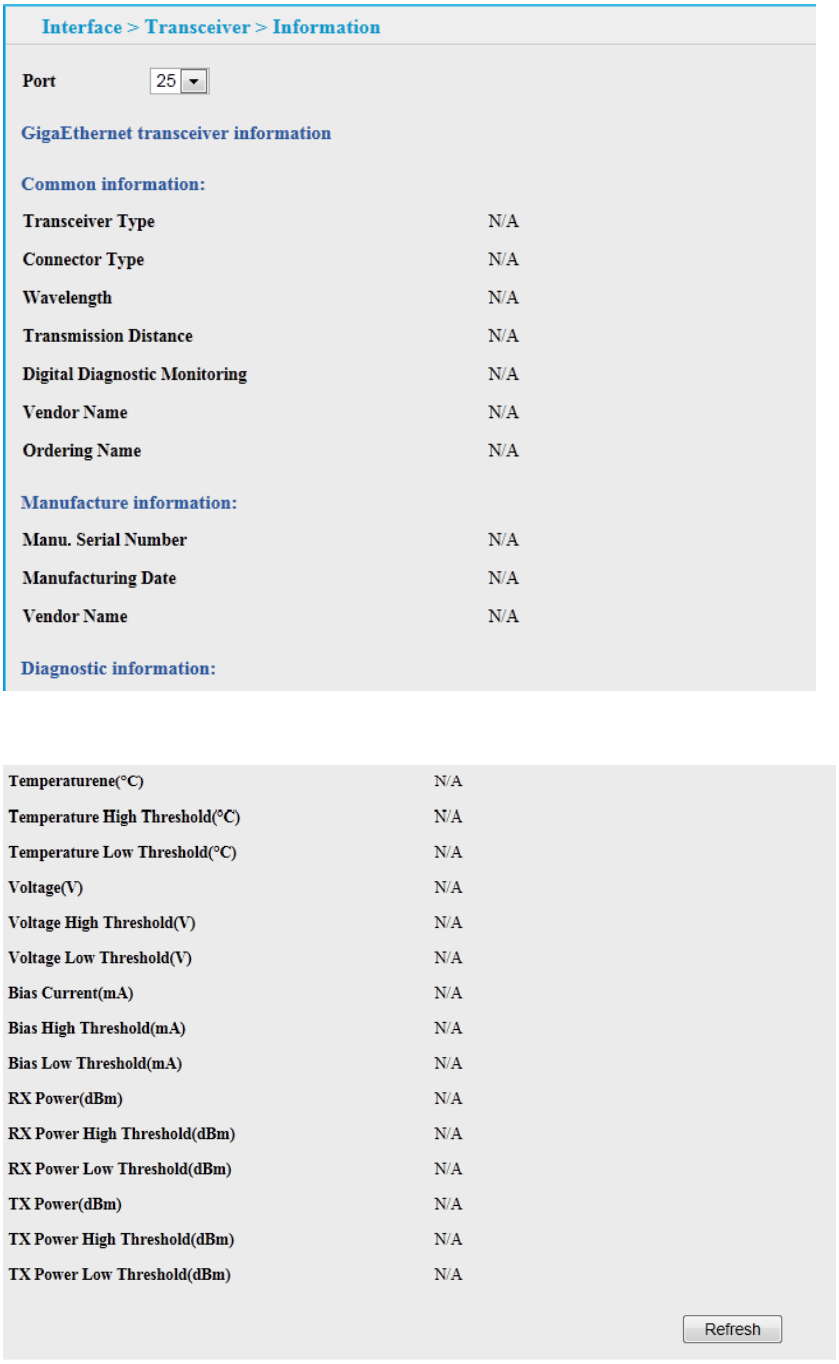
Title	Description
Received Octets	The total number of octets received on the interface, including framing characters.
Transmitted Octets	The total number of octets transmitted out of the interface, including framing characters.
Received Unicast Packets	The total number of received unicast packets.
Transmitted Unicast Packets	The total number of transmitted unicast packets.
Received Multicast Packets	The total number of received multicast packets.
Transmitted Multicast Packets	The total number of transmitted multicast packets.
Received Broadcast Packets	The total number of received broadcast packets.
Transmitted Broadcast Packets	The total number of transmitted broadcast packets.

----End

4.3 Transceiver

Use the Interface > Transceiver > Information page to show the transceiver information on the selected port.

Figure 4-16 Showing Transceiver Information



4.4 Power Saving

Use the Interface > Green Ethernet page to enable power savings mode on the selected port.

To enable power savings:

1. Click Interface > Green Ethernet.
2. Mark the Enabled check box for a port.

3. Click Apply.

Figure 4-17 Enabling Power Savings

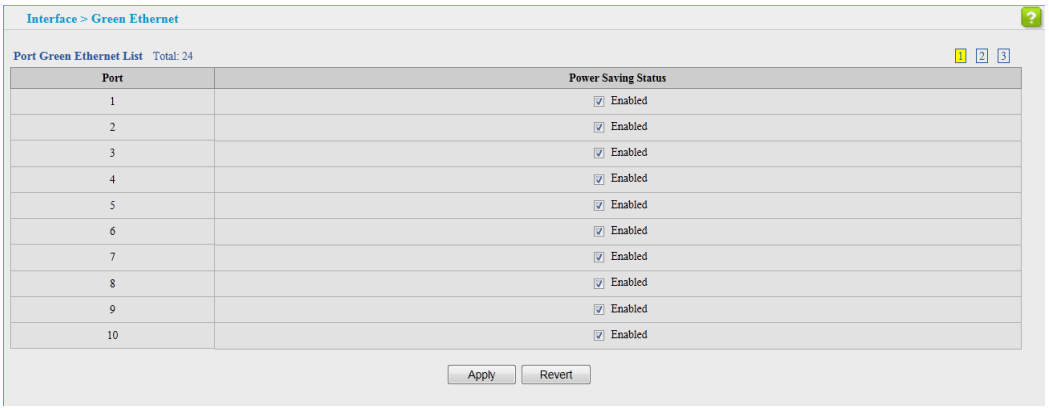


Table 4-8 Parameters of Green Ethernet

Title	Description
Port	Power saving mode only applies to the Gigabit Ethernet ports using copper media.
Power Saving Status	Adjusts the power provided to ports based on the length of the cable used to connect to other devices. Only sufficient power is used to maintain connection requirements. (Default: Enabled on Gigabit Ethernet RJ-45 ports)

----End

5 VLAN Configuration

About This Chapter

The following sections describe how to configure and query VLAN and interface information. A local area network can be devided into several logical LANs. Each logical LAN is a broadcast domain, which is called a virtual LAN (VLAN). To put it simply, deveices on a LAN are logically grouped into different LAN segments, regardless of their pgysical locations. VLANs isolate broadcast domains on a LAN.

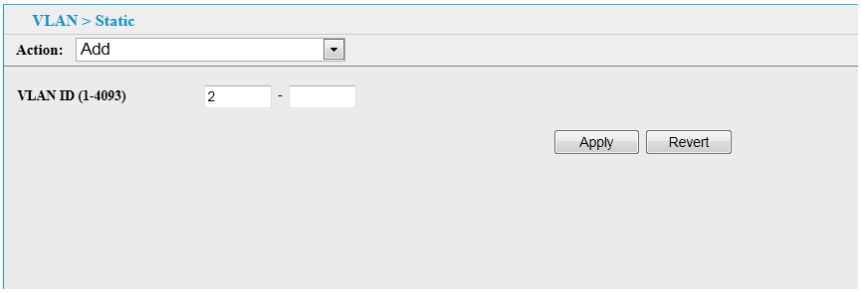
5.1 Configuring Static VLAN

Use the VLAN > Static (Configure VLAN) page to create or remove VLAN, modify VLAN, edit/show member by VLAN, edit/show member by interface, edit/show member by interface range. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

5.1.1 Creating a Static VLAN

1. Click VLAN > Static. Select Add from the Action list. Figure 5-1 is displayed.

Figure 5-1 Creating Static VLANs



2. Enter a VLAN ID or range of IDs. See Table 5-1 for the parameters description.

Table 5-1 Parameters of Creating Static VLANs

Title	Description
VLAN ID	ID of VLAN or range of VLANs (1-4093). Up to 256 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.

3. Click Apply.

CAUTION

System can be configured 256 VLANs. VLAN1 is the default untagged VLAN.

----End

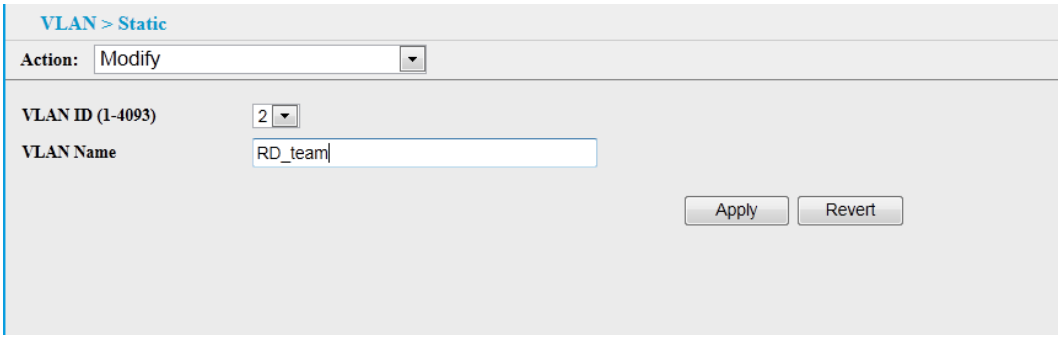
5.1.2 Adding Static Members to VLANs

Use the VLAN > Static (Edit Member By Vlan), Edit Member by Interface, or Edit Member by Interface Range) pages to configure port members for the selected VLAN index, interface, or a range of interfaces. Use the menus for editing port members to configure the VLAN behavior for specific interfaces, including the mode of operation (Hybrid, 1Q Trunk or Access), the default VLAN identifier (PVID), accepted frame types, and ingress filtering. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLANaware devices.

5.1.3 Modify VLAN

1. Click VLAN > Static. Select Modify from the Action list. Figure 5-2 is displayed.

Figure 5-2 Modifying Static VLAN



2. Select the VLAN ID need to modify. Enter a VLAN Name. See Table 5-2.

Table 5-2 Parameters of modifying VLAN

Title	Description
VLAN ID	ID of VLAN or range of VLANs (1-4093). Up to 256 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.
VLAN Name	Name of the VLAN.

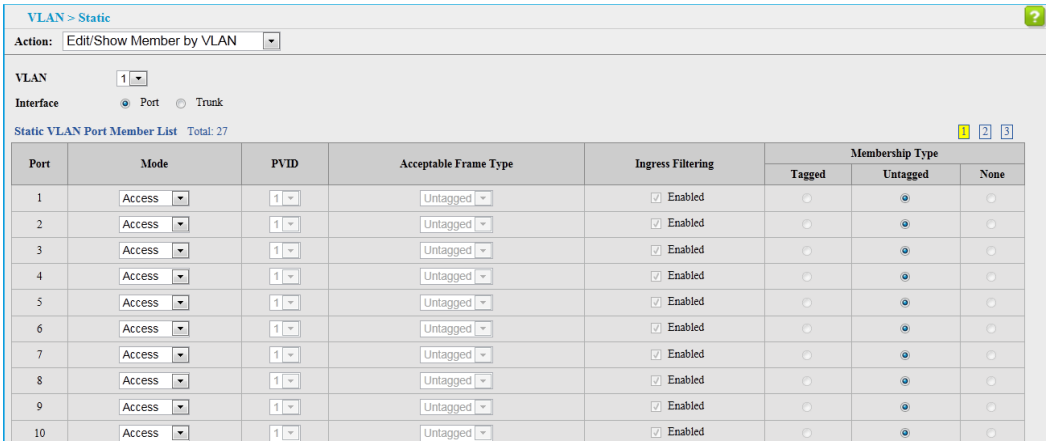
3. Click Apply.

----End

5.1.4 Edit/Show Member by VLAN

1. Click VLAN > Static. Select Edit/Show Member by VLAN from the Action list. Figure 5-3 is displayed.

Figure 5-3 Editing/Showing Static Members by VLAN Index



2. Set the Interface type to display as Port or Trunk.
3. Modify the settings for any interface as required. Remember that Membership Type cannot be changed until an interface has been added to another VLAN and the PVID changed to anything other than 1. SeeTable 5-3.
4. Click Apply.

Table 5-3 Parameters of Configuring Static Members by VLAN Index

Title	Description
VLAN	ID of configured VLAN (1-4093).
Interface	Displays a list of ports or trunks.
Port	Port Identifier(1-28).

Title	Description
Trunk	Trunk Identifier. (Range: 1-12)
Mode	Indicates VLAN membership mode for an interface. (Default: Access) • Access: Sets the port as an Access VLAN interface. The port transmits and receives untagged frames on a single VLAN only. • Hybrid: Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames. • 1Q Trunk: Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as untagged frames.
PVID	VLAN ID assigned to untagged frames received on the interface. (Default: 1) When using Access mode, and an interface is assigned to a new VLAN, its PVID is automatically set to the identifier for that VLAN. When using Hybrid mode, the PVID for an interface can be set to any VLAN for which it is an untagged and tagged member.
Acceptable Frame Type	Sets the interface as to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Options: All, Tagged, Untagged; Default: All) Acceptalbe Frame Type not supported under access mode.
Ingress Filtering	Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Enabled) • Ingress filtering only affects tagged frames. • If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port). • If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded. • Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP. The frame type is acceptable here into the direction with tagged, here configured with tagged, but the configuration interface PVID must specify whether 1 or 4093, there has been specified with tagged, so PVID should not come into force, this is only forin the inbound direction.

Title	Description
Membership Type	Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk: • Tagged: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information. • Untagged: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port. • None: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.

CAUTION

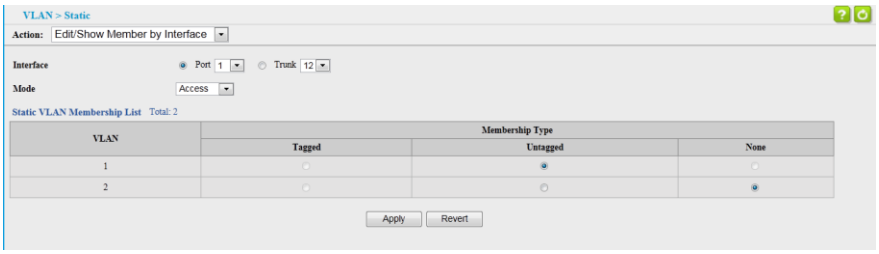
VLAN 1 is the default untagged VLAN, including all the ports of the switch and the mode used is Access.

----End

5.1.5 Edit/Show member by interface

1. Click VLAN > Static. Select Edit/Show Member by Interface from the Action list. Figure 5-4 is displayed.

Figure 5-4 Editing/Showing Static Members by Interface



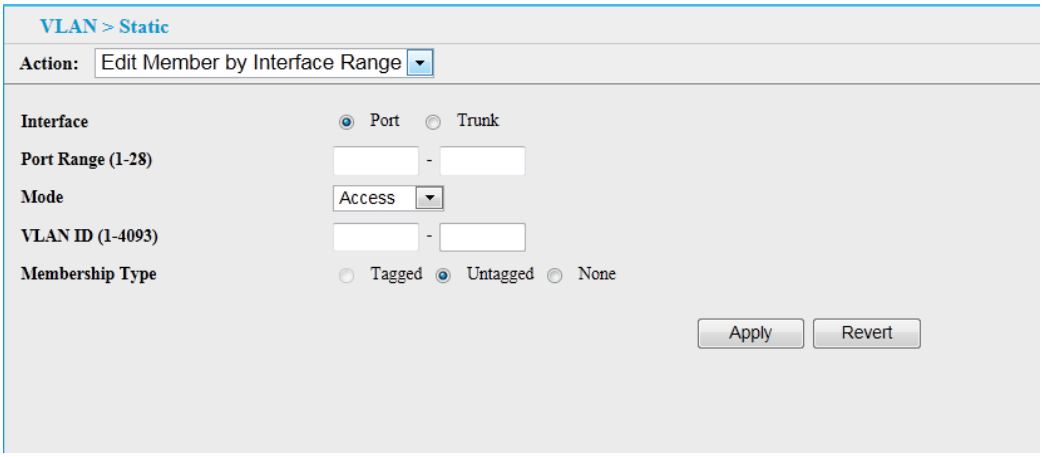
2. Select a port or trunk configure.
3. Modify the settings for any interface as required. SeeTable 5-3.
4. Click Apply.

----End

5.1.6 Edit/Show member by interface range

1. Click VLAN > Static. Select Edit Member by Interface Range from the Action list. Figure 5-5 is displayed.

Figure 5-5 Configuring Static Members by Interface Range



2. Set the Interface type to display as Port or Trunk.
3. Enter an interface range.
4. Modify the VLAN parameters as required. Remember that the PVID, acceptable frame type, and ingress filtering parameters for each interface within the specified range must be configured on either the Edit Member by VLAN or Edit Member by Interface page. See Table 5-3, Table 5-4.
5. Click Apply.

Table 5-4 Parameters of Configuring Static Members by Interface Range

Title	Description
Port Range	Displays a list of port range (1-28).
Trunk Range	Displays a list of Trunk range (1-12).

CAUTION

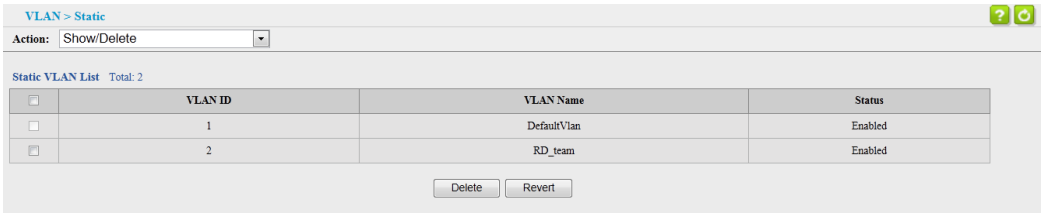
Withing the specified interface range, the PVID of every interface, Acceptable Frame Type, and Ingress Filtering must be set in the page Edit/Show Member by VLAN and Edit/Show Member by Interface.

----End

5.1.7 Show/delete Static VLAN

1. Click VLAN > Static. Select Show/Delete from the Action list to view static VLAN. See Figure 5-6.

Figure 5-6 Showing/Deleting Static VLANs



2. Select the VLAN ID need to be deleted, and then click Delte to delete the static VLAN.

----End

6 MAC Address Configuration

About This Chapter

6.1 Setting Static Address

Use the MAC Address > Static page to configure static MAC addresses. A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be aging. When an address is seen on another interface, the address will be ignored and will not be written to the address table.

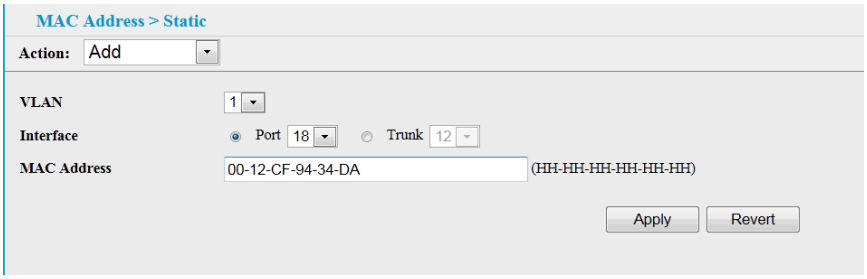
The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics in a specific VLAN :

- Static addresses are bound to the assigned interface and will not be aging. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- A static address cannot be learned on another port until the address is removed from the table manually.

To add static MAC address:

1. Click MAC Address > Static. Select Add from the Action list.
2. Specify the VLAN, the port or trunk to which the address will be assigned, and the MAC address. See Figure 6-1.
3. Click Apply.

Figure 6-1 Adding Static MAC Addresses



----End

To show/delete the static addresses in MAC address table:

1. Click MAC Address > Static. Select Show/Delete from the Action list to view the static MAC Addresses. See Figure 6-2.

Figure 6-2 Showing/Deleting Static MAC Addresses

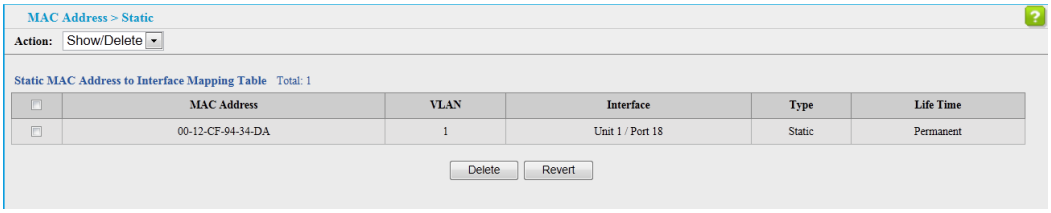


Table 6-1 Parameters of Static MAC Address

Title	Description
MAC Address	Physical address of a device mapped to this interface. Enter an address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.
VLAN	ID of configured VLAN. (Range: 1-4093)
Interface	Port or trunk associated with the device assigned a static address.
Type	Means that the entries in this table are static.
Life Time	The time to retain for the specific address. • Delete-on-reset - Assignment lasts until the switch is reset. • Permanent - Assignment is permanent. (This is the default.)

2. Select the MAC Address need to be deleted, and then clock Delete to delete the MAC Address.

----End

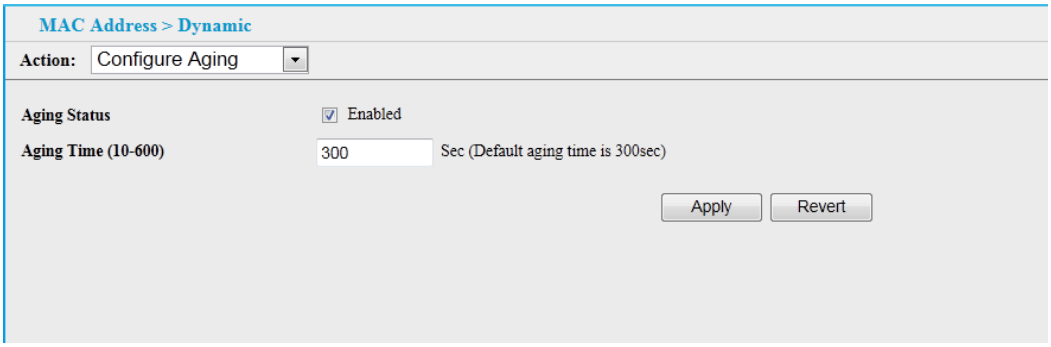
6.2 Setting Dynamic Address

6.2.1 Changing the Aging Time

Use the MAC Address > Dynamic (Configure Aging) page to set the aging time for entries in the dynamic address table. The aging time is used to age out dynamically learned forwarding information.

1. Click MAC Address > Dynamic. Select Configure Aging from the Action list. See Figure 6-3.

Figure 6-3 Setting the Address Aging Time



These parameters are displayed in the web interface:

- Aging Status – Enables/disables the function.
- Aging Time – The time after which a learned entry is discarded. (Range: 10-600 seconds; Default: 300 seconds)

2. Modify the aging status if required. Specify a new aging time.
3. Click Apply.

----End

6.2.2 Displaying the Dynamic Address Table

Use the MAC Address > Dynamic (Show Dynamic MAC) page to display the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

1. Click MAC Address > Dynamic. Select Show Dynamic MAC from the Action list.

Figure 6-4 Displaying the Dynamic MAC Address Table

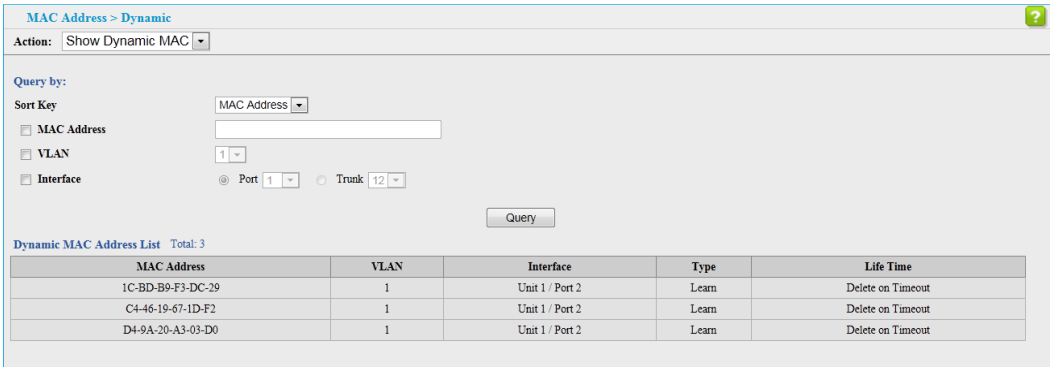


Table 6-2 Parameters of Displaying the Dynamic MAC Address

Title	Description
Sort Key	You can sort the information displayed based on MAC address, VLAN or interface (port or trunk).
MAC Address	Physical address associated with interface.
VLAN	ID of configured VLAN (1-4093).
Interface	Indicates a port or trunk.
Type	Means that the entries in this table are learned.
Life Time	The overall life time to retain the specified address.

2. Select the Sort Key (MAC Address, VLAN, or Interface). Enter the search parameters (MAC Address, VLAN, or Interface).
3. Click Query.

----End

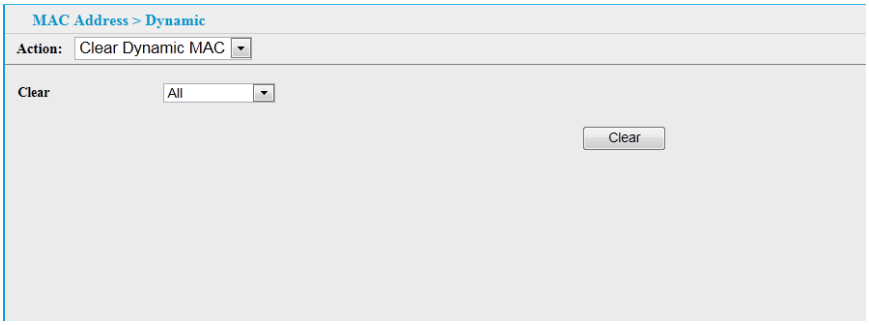
6.2.3 Clearing the Dynamic Address Table

Use the MAC Address > Dynamic (Clear Dynamic MAC) page to remove any learned entries from the forwarding database.

To clear the entries in the dynamic address table:

1. Click MAC Address > Dynamic. Select Clear Dynamic MAC from the Action list. See Figure 6-5.
2. Select the method by which to clear the entries (i.e., All, MAC Address, VLAN, or Interface).
3. Set the information required for clearing entries by MAC Address, VLAN, or Interface.
4. Click Clear.

Figure 6-5 Clearing Ehtries in the Dynamic MAC Address Table



These parameters are displayed in the web interface:

- Clear by – All entries can be cleared; you can clear the entries for a specific MAC address, all the entries in a VLAN; all the entries associated with a port or trunk.

----End

7 Spanning Tree Algorithm

About This Chapter

7.1 Configuring Global STP

Use the Spanning Tree > STP (Configure Global - Configure) page to configure global settings for the spanning tree that apply to the entire switch.

To configure global STP settings:

1. Click Spanning Tree, STP.
2. Select Configure Global from the Step list.
3. Select Configure from the Action list.
4. Modify any of the required attributes.
5. Click Apply.

Figure 7-1 Configuring Global Settings for STP (STP)

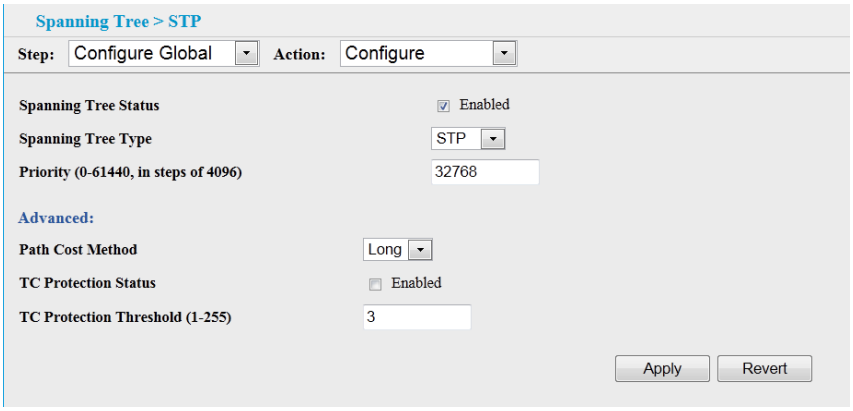


Figure 7-2 Configuring Global Settings for STP (RSTP)

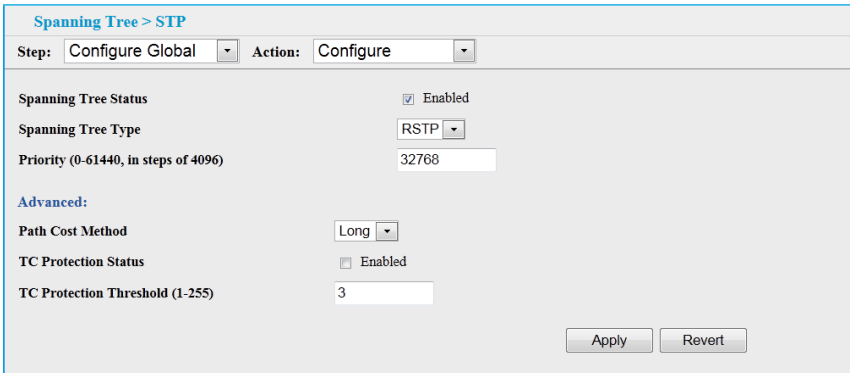


Table 7-1 Parameters of Global Settings for STP

Title	Description
Basic Configuration of Global Settings	
SpanningTree Status	Enables/disables STP on this switch. (Default: Enabled)
Spanning Tree Type	Specifies the type of spanning tree used on this switch: • STP: Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode). • RSTP: Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.

Title	Description
Priority	Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.) • Default: 32768 • Range: 0-61440, in steps of 4096 • Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.
The following attributes are based on RSTP, but also apply to STP since the switch uses a backwards-compatible subset of RSTP to implement STP:	
Advanced Configuration Settings	
Path Cost Method	The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface. • Long: Specifies 32-bit based values that range from 1-200,000,000. (This is the default.) • Short: Specifies 16-bit based values that range from 1-65535.
TC Protection Status	Switch will operate on MAC deleting continuly if meets TC attacking, this will affect packet forwarding. User can configure the operating sequency of BPDU packet to avoid TC-BPDU attacking.
TC Protection Threshold (1-255)	The threshold time needed by TC.3 times in 2s at default. The configuratable time range is 1-255.

----End

7.2 Showing Global Settings for STP

Use the Spanning Tree > STP (Configure Global - Show Information) page to display a summary of the current bridge STP information that applies to the entire switch.

To display global STP settings:

1. Click Spanning Tree, STP.
2. Select Configure Global from the Step list.
3. Select Show Information from the Action list.

Figure 7-3 Displaying Global Settings for STP

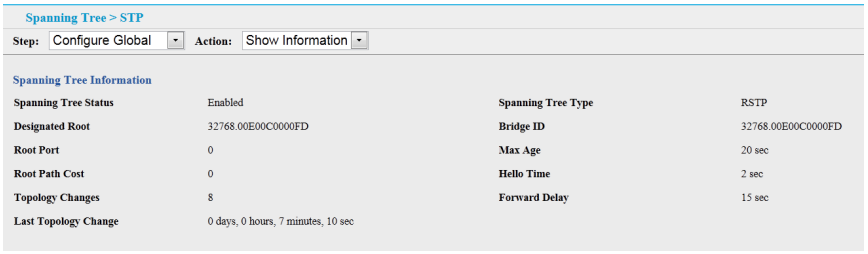


Table 7-2 More Parameters of Global Settings for STP

Title	Description
Bridge ID	A unique identifier for this bridge, consisting of the bridge priority, and MAC address (where the address is taken from the switch system).
Designated Root	The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
Root Port	The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
Root Path Cost	The path cost from the root port on this switch to the root device.
Topology changes	The number of times the Spanning Tree has been reconfigured.
Last Topology Change	Time since the Spanning Tree was last reconfigured.
Hello Time	Interval (in seconds) at which the root device transmits a configuration message. • Default: 2 • Minimum: 1 • Maximum: The lower of 10 or [(Max. Message Age / 2) -1]
Max Age	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. • Default: 20 • Minimum: The higher of 6 or [2 x (Hello Time + 1)] • Maximum: The lower of 40 or [2 x (Forward Delay - 1)]

Title	Description
Forward Delay	The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result. • Minimum: The higher of 4 or [(Max. Age / 2) + 1] • Maximum: 30

----End

7.3 Configuring Interface Settings for STP

Use the Spanning Tree > STP (Configure Interface - Configure) page to configure RSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or sharedmedia connection, and edge port to indicate if the attached device can support fast forwarding. (References to "ports" in this section means "interfaces," which includes both ports and trunks.)

To configure interface settings for STP:

1. Click Spanning Tree, STP.
2. Select Configure Interface from the Step list.
3. Select Configure from the Action list.
4. Modify any of the required attributes.
5. Click Apply.

Figure 7-4 Configuring Interface Settings for STP

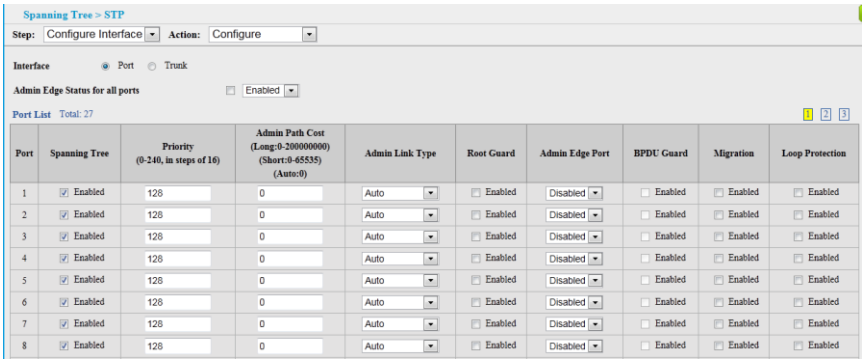


Table 7-3 Parameters of STP

Title	Description
Interface	Displays a list of ports or trunks.
Admin Edge Status for all ports	Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate econfiguration when the interface changes state, and also overcomes other STP-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Enabled) • Enabled – Manually configures a port as an Edge Port. • Disabled – Disables the Edge Port setting.
Spanning Tree	Enables/disables STP on this interface. (Default: Enabled)
Priority	Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. • Default: 128 • Range: 0-240, in steps of 16
Admin Path Cost	This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost takes precedence over port priority. (Range: 0 for auto-configuration, 1-65535 for the short path cost method3, 1-200,000,000 for the long path cost method)
Admin Link Type	The link type attached to this interface. • Point-to-Point – A connection to exactly one other bridge. • Shared – A connection to two or more bridges. • Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)
Root Guard	STP allows a bridge with a lower bridge identifier (or same identifier and lower MAC address) to take over as the root bridge at any time. Root Guard can be used to ensure that the root bridge is not formed at a suboptimal location. Root Guard should be enabled on any designated port connected to low-speed bridges which could potentially overload a slower link by taking over as the root port and forming a new spanning tree topology. It could also be used to form a border around part of the network where the root bridge is allowed. (Default: Disabled)
Admin Edge Por	Refer to “Admin Edge Status for all ports” at the beginning of this section.

Title	Description
BPDU Guard	This feature protects edge ports from receiving BPDUs. It prevents loops by shutting down an edge port when a BPDU is received instead of putting it into the spanning tree discarding state. In a valid configuration, configured edge ports should not receive BPDUs. If an edge port receives a BPDU an invalid configuration exists, such as a connection to an unauthorized device. The BPDU guard feature provides a secure response to invalid configurations because an administrator must manually enable the port. (Default: Disabled)
Migration	If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STPcompatible) to send on the selected interfaces. (Default: Disabled)
Loop Protection	Enable/disable Loop Protection

----End

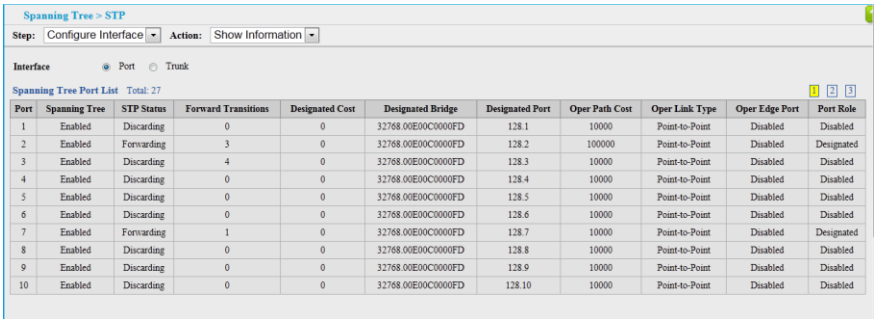
7.4 Displaying Interface Settings for STP

Use the Spanning Tree > STP (Configure Interface - Show Information) page to display the current status of ports or trunks in the Spanning Tree.

To display interface settings for STP:

1. Click Spanning Tree, STP.
2. Select Configure Interface from the Step list.
3. Select Show Information from the Action list.

Figure 7-5 Displaying Interface Settings for STP



Port	Spanning Tree	STP Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role
1	Enabled	Discarding	0	0	32768.00E00C0000FD	128.1	10000	Point-to-Point	Disabled	Disabled
2	Enabled	Forwarding	3	0	32768.00E00C0000FD	128.2	100000	Point-to-Point	Disabled	Designated
3	Enabled	Discarding	4	0	32768.00E00C0000FD	128.3	10000	Point-to-Point	Disabled	Disabled
4	Enabled	Discarding	0	0	32768.00E00C0000FD	128.4	10000	Point-to-Point	Disabled	Disabled
5	Enabled	Discarding	0	0	32768.00E00C0000FD	128.5	10000	Point-to-Point	Disabled	Disabled
6	Enabled	Discarding	0	0	32768.00E00C0000FD	128.6	10000	Point-to-Point	Disabled	Disabled
7	Enabled	Forwarding	1	0	32768.00E00C0000FD	128.7	10000	Point-to-Point	Disabled	Designated
8	Enabled	Discarding	0	0	32768.00E00C0000FD	128.8	10000	Point-to-Point	Disabled	Disabled
9	Enabled	Discarding	0	0	32768.00E00C0000FD	128.9	10000	Point-to-Point	Disabled	Disabled
10	Enabled	Discarding	0	0	32768.00E00C0000FD	128.10	10000	Point-to-Point	Disabled	Disabled

Table 7-4 Parameters of Displaying Interface Settongs for STP

Title	Description
Spanning Tree	Shows if STP has been enabled on this interface.
STP Status	Displays current state of this port within the Spanning Tree: • Discarding - Port receives STP configuration messages, but does not forward packets. • Learning - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses. • Forwarding - Port forwards packets, and continues learning addresses.
Forward Transitions	The number of times this port has transitioned from the Learning state to the Forwarding state
Designated Cost	The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media,the higher the cost.
Designated Bridge	The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
Designated Port	The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
Oper Path Cost	The contribution of this port to the path cost of paths towards the spanning tree root which include this port.
Oper Link Type	The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection,
Oper Edge Port	This parameter is initialized to the setting for Admin Edge Port in STP Port Configuration (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
Port Role	Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (i.e., root port), connecting a LAN through the bridge to the root bridge (i.e., designated port), is the MSTI regional root (i.e., master port), or is an alternate or backup port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., disabled port) if a port has no role within the spanning tree.

----End

8 Rate Limit Configuration

About This Chapter

8.1 Configuring Rate Limit

Use the Traffic > Rate Limit page to apply rate limiting to egress ports. This function allows the network manager to control the maximum rate for traffic transmitted on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic out of the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

To configure rate limits:

1. Click Traffic, Rate Limit.
2. Enable the Rate Limit Status for the required ports.
3. Set the rate limit for the individual ports,.
4. Click Apply.

Figure 8-1 Configuring Rate Limits

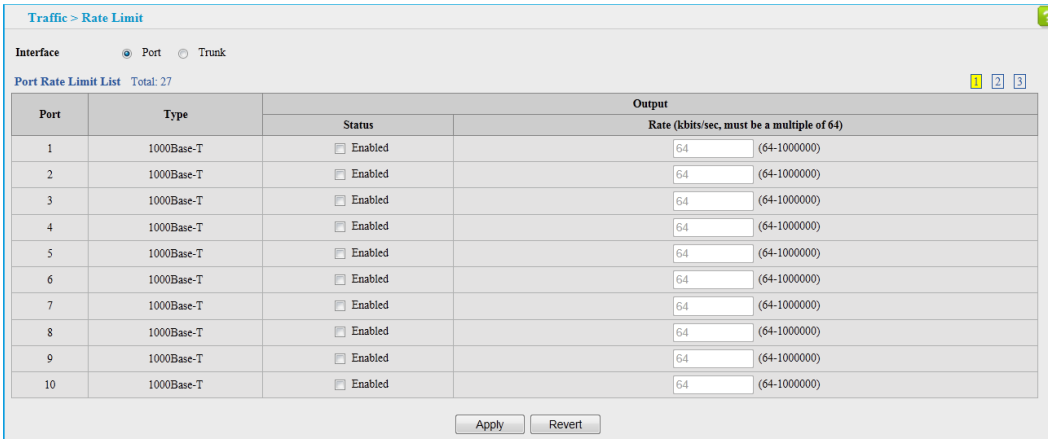


Table 8-1 Parameters of Rate Limits

Title	Description
Port	Displays the port number.
Type	Indicates the port type. (1000Base-T, or 1000Base SFP)
Status	Enables or disables the rate limit. (Default: Disabled)
Rate	Sets the rate limit level. (Range: 64 - 1,000,000 kbits per second for Gigabit Ethernet ports)

----End

8.2 Configuring Storm Control

Use the Traffic > Storm Control page to configure broadcast, multicast, and unknown unicast storm control thresholds. Traffic storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from traffic storms by setting a threshold for broadcast, multicast or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped.

To configure broadcast storm control:

1. Click Traffic, Storm Control.
2. Set the Status field to enable or disable storm control.
3. Set the required threshold beyond which the switch will start dropping packets.
4. Click Apply.

Figure 8-2 Configuring Storm Control

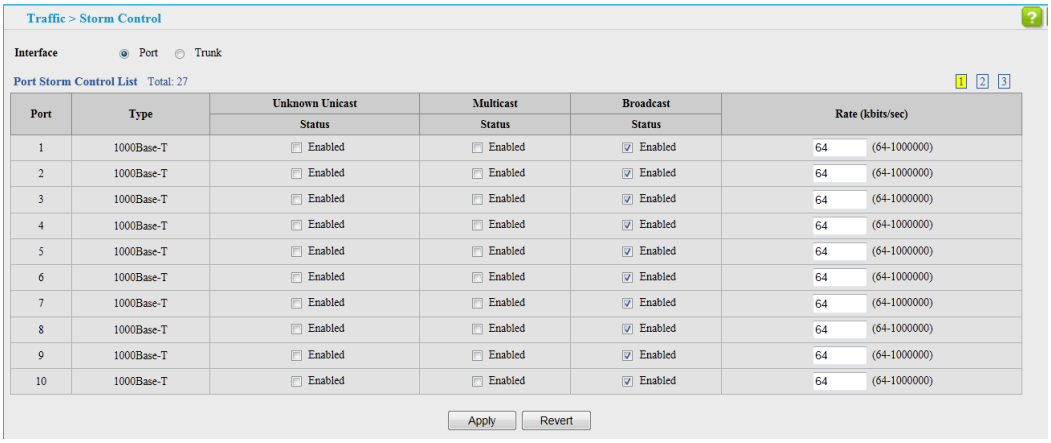


Table 8-2 Parameters of Configuring Storm Control

Title	Description
Interface	Displays a list of ports or trunks.
Type	Indicates interface type. (1000Base-T, or 1000Base SFP)
Unknown Unicast	Specifies storm control for unknown unicast traffic.
Multicast	Specifies storm control for multicast traffic.
Broadcast	Specifies storm control for broadcast traffic.
Status	Enables or disables storm control. (Default:Unknown Unicast Disabled; Multicast Disabled; Broadcast Enabled)
Rate	Threshold level as a rate; i.e., kilobits per second. (Range: 64-1000000 Kbps for Gigabit Ethernet ports)

----End

8.3 Configuring Class of Service

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

8.3.1 Setting the Default Priority for Interface

Use the Traffic > Priority > Default Priority page to specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

- This switch provides four priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage, but can be configured to process each queue in strict order, or use a combination of strict and weighted queueing.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.

To configure the Default Priority of ports:

1. Click Traffic, Priority, Default Priority.
2. Select the interface type to display (Port or Trunk).
3. Modify the default priority for any interface.
4. Click Apply.

Figure 8-3 Setting the Default Port Priority

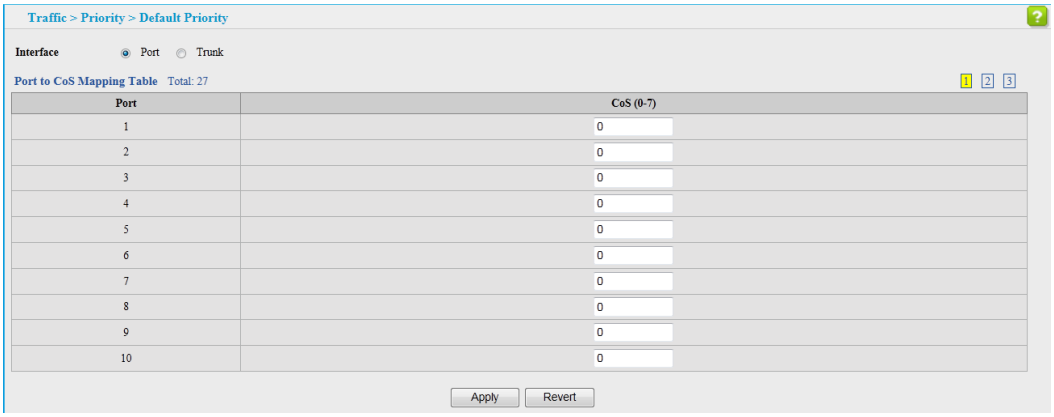


Table 8-3 Parameters of Default Port Priority

Title	Description
Interface	Displays a list of ports or trunks.
CoS	The priority that is assigned to untagged frames received on the specified interface. (Range: 0-7; Default: 0)

----End

8.3.2 Selecting the Queue Mode

Use the Traffic > Priority > Queue page to set the queue mode for the egress queues on any interface. The switch can be set to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before the lower priority queues are serviced, Shaped Deficit Weighted Round-Robin (SDWRR) queuing that specifies a scheduling weight for each queue. SDWRR is labelled WRR in the menu. It can also be configured to use a combination of strict and weighted queuing.

To configure the queue mode:

1. Click Traffic, Priority, Queue.
2. Set the queue mode.
3. If the weighted queue mode is selected, the queue weight can be modified if required.
4. If the queue mode that uses a combination of strict and weighted queueing is selected, the queues which are serviced first must be specified by enabling strict mode parameter in the table.
5. Click Apply.

Figure 8-4 Setting the Queue Mode(Strict)

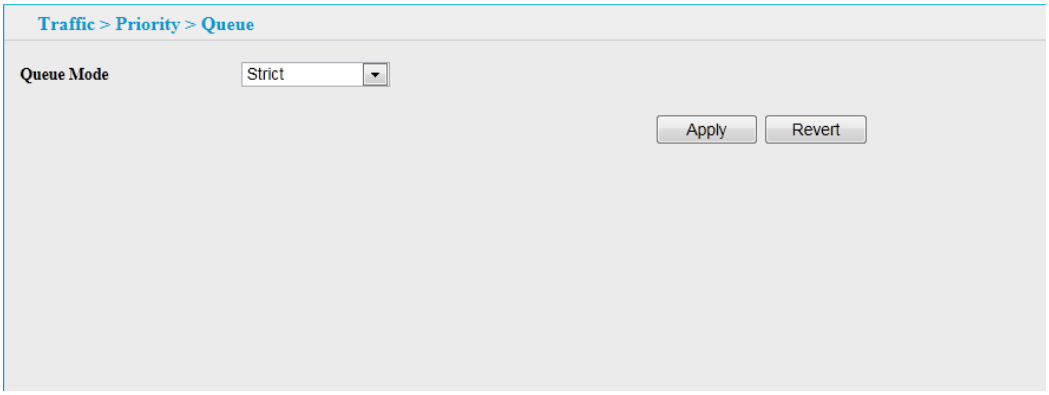


Figure 8-5 Setting the Queue Mode(WRR)

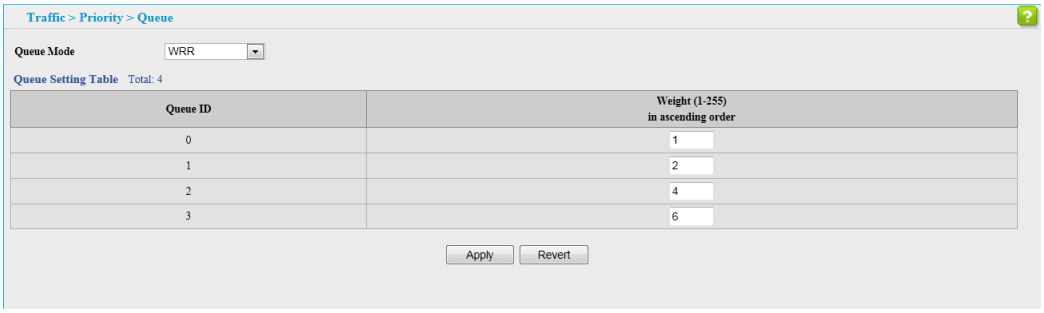


Figure 8-6 Setting the Queue Mode(Strict & WRR)

Table 8-4 Parameters of Queue Mode

Title	Description
Queue Mode	• Strict – Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic. • WRR– Shares bandwidth at the egress ports by using scheduling weights, servicing each queue in a round-robin fashion. • Strict and WRR – Uses strict priority on the high-priority queues and SDWRR for the rest of the queues. (This is the default setting.)
Queue ID	The ID of the priority queue. (Range: 0-3)
Strict Mode	If "Strict and WRR" mode is selected, then a combination of strict service is used for the high priority queues and weighted service for the remaining queues. Use this parameter to specify the queues assigned to use strict priority when using the strictweighted queuing mode. (Default: Strict and WRR mode, with Queue 3 using strict mode)
Weight	Sets a weight for each queue which is used by the SDWRR scheduler. (Range: 1-255; Default: Weights 1, 2, 4, 6 are assigned to queues 0 - 3 respectively)

----End

8.3.3 Configuring Trust Mode

Use the Traffic > Priority >Trust mode page to set the trust mode. Trust mode is used to select the way which the priority of the packet mapping to the internal priority of device.When trust mode is CoS, the priority of packet with VLAN tag will be used to map tp internal priority. When trust mode is DSCP, if packet is IP packet, DCSP of packet will be used to map internal priority, for non-IP packet, the priority of packet with VLAN tag will be used to map internal priority. The internal priority of device decides the final submit queue entering the hardware. By default, trust mode is DSCP.

To configure the trust mode:

1. Click Traffic, Priority, Trust Mode.
2. Select the interface type to display (Port or Trunk).
3. Set the trust mode.
4. Click Apply.

Figure 8-7 Setting the Trust Mode

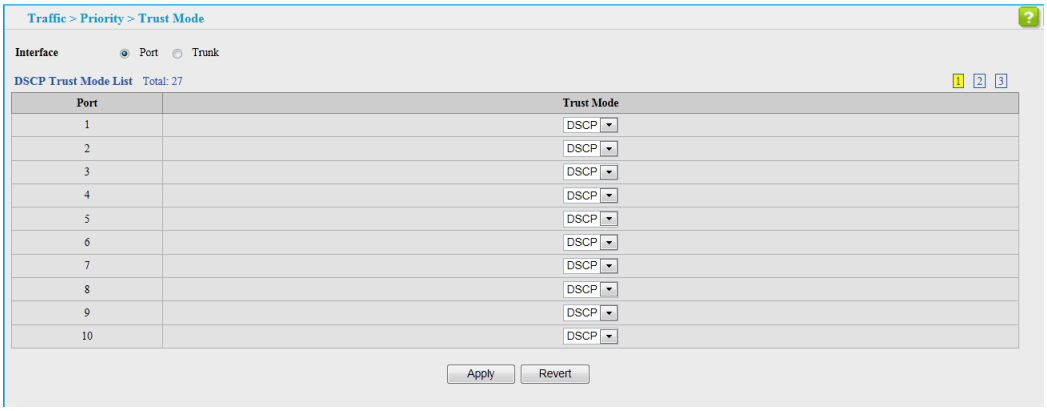


Table 8-5 Parameters of Trust Mode

Title	Description
Interface	Specifies a port or trunk.
Trust Mode	• DSCP – Maps layer 3/4 priorities using Differentiated Services Code Point values. • CoS – Maps layer 3/4 priorities using Class of Service values. (This is the default setting.)

----End

8.3.4 Mapping Ingress DSCP Values to PHB

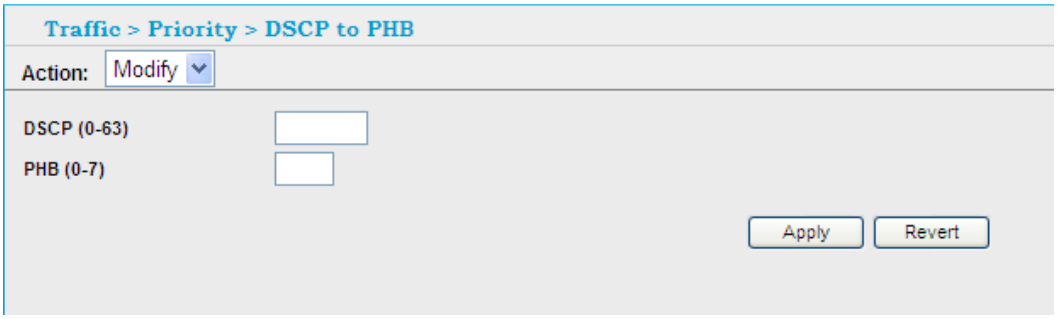
Use the Traffic > Priority > DSCP to PHB page to map DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing.

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

To map DSCP values to internal PHB:

1. Click Traffic, Priority, DSCP to PHB.
2. Select Modify from the Action list.
3. Set the PHB for any DSCP value.
4. Click Apply.

Figure 8-8 Configuring DSCP to PHB



----End

To show the DSCP to internal PHB map:

1. Click Traffic, Priority, DSCP to PHB.
2. Select Show from the Action list.

Figure 8-9 Showing DSCP to PHB

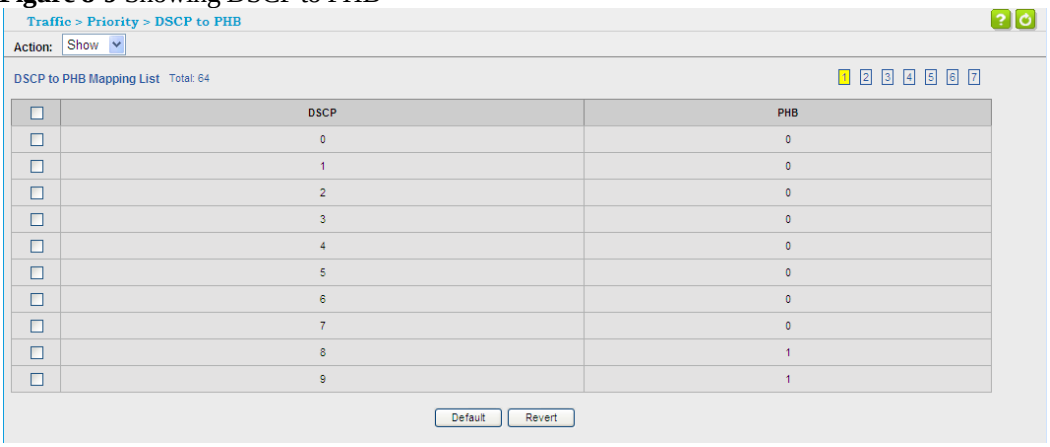


Table 8-6 Parameters of DSCP to PHB

Title	Description
DSCP	DSCP value in ingress packets. (Range: 0-63)
PHB	Per-hop behavior, or the priority used for this router hop.(Range: 0-7)

----End

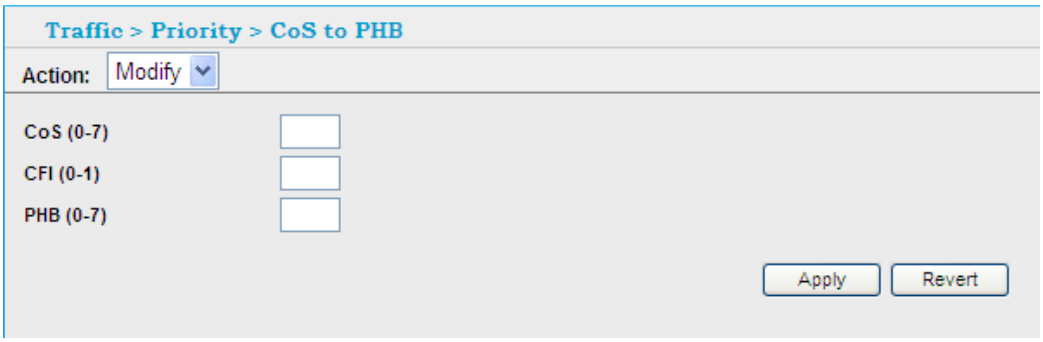
8.3.5 Mapping CoS Priorities to PHB

Use the Traffic > Priority > CoS to PHB page to maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing.

To map CoS/CFI values to internal PHB:

1. Click Traffic, Priority, CoS to PHB.
2. Select Modify from the Action list.
3. Set the PHB for any of the CoS/CFI combinations.
4. Click Apply.

Figure 8-10 Configuring CoS to PHB



----End

To show the CoS/CFI to internal PHB map:

1. Click Traffic, Priority, CoS to PHB.
2. Select Show from the Action list.

Figure 8-11 Showing CoS to PHB

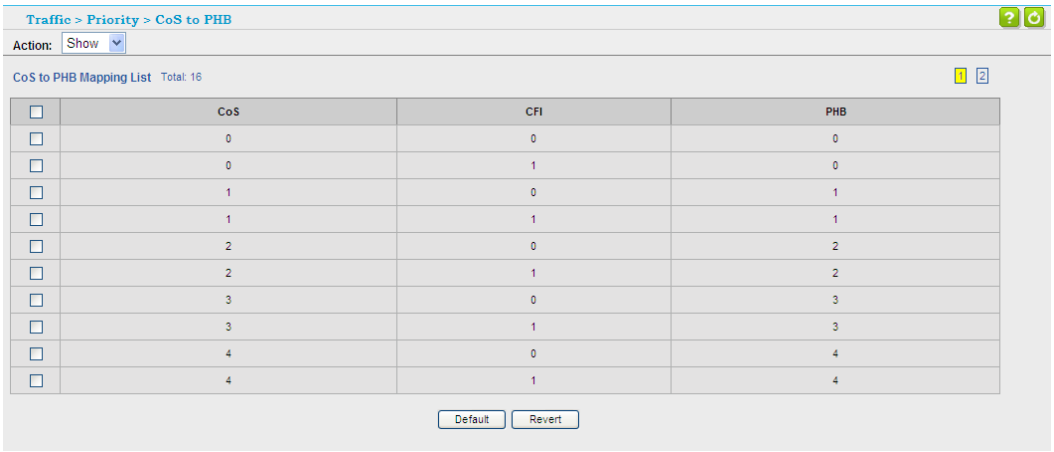


Table 8-7 Parameters of CoS to PHB

Title	Description
CoS	CoS value in ingress packets. (Range: 0-7)

Title	Description
CFI	Canonical Format Indicator. Set this parameter to “0” to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)
PHB	Per-hop behavior, or the priority used for this router hop.(Range: 0-7)

----End

8.3.6 Mapping PHB Values to Queues

Use the Traffic > Priority > PHB to Queue page to specify the hardware output queues to use based on the internal per-hop behavior value. (For more information on exact manner in which the ingress priority tags are mapped to egress queues for internal processing.)

The switch processes Class of Service (CoS) priority tagged traffic by using four priority queues for each port, with service schedules based on strict priority, Shaped Deficit Weighted Round-Robin (SDWRR), or a combination of strict and weighted queuing. Up to eight separate traffic priorities are defined in IEEE 802.1p. Default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in Table 8-8. This table indicates the default mapping of internal per-hop behavior to the hardware queues. The actual mapping may differ if the CoS priorities to internal DSCP values have been modified.

Table 8-8 IEEE802.1p Egress Queue Priority Mapping

Priority	0	1	2	3	4	5	6	7
Queue	1	0	0	1	2	2	3	3

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown inTable 8-9. However, priority levels can be mapped to the switch’s output queues in any way that benefits application traffic for the network.

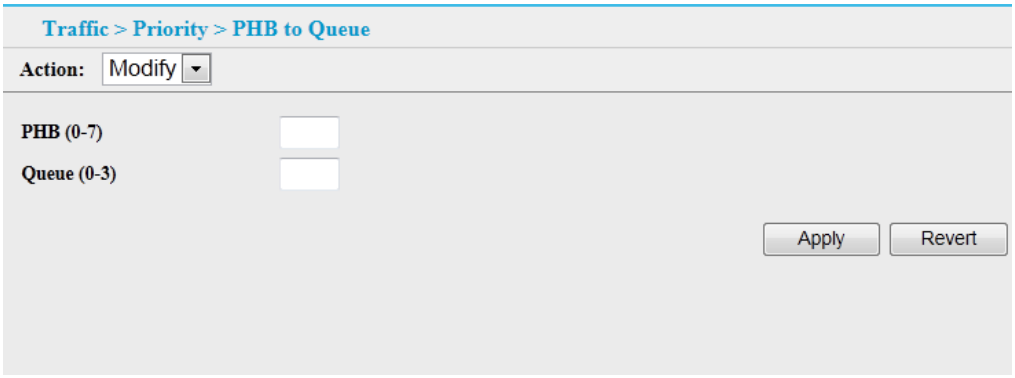
Table 8-9 CoS Priority Levels

Priority Level	Traffic Type
1	Background
2	(Spare)
0	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

To map internal PHB to hardware queues:

1. Click Traffic, Priority, PHB to Queue.
2. Select Add from the Action list.
3. Map an internal PHB to a hardware queue.
4. Click Apply.

Figure 8-12 Mapping PHB Value to Queues



----End

To show the internal PHB to hardware queue map:

1. Click Traffic, Priority, PHB to Queue.
2. Select Show from the Action list.

Figure 8-13 Showing PHB Value to Queue Mapping

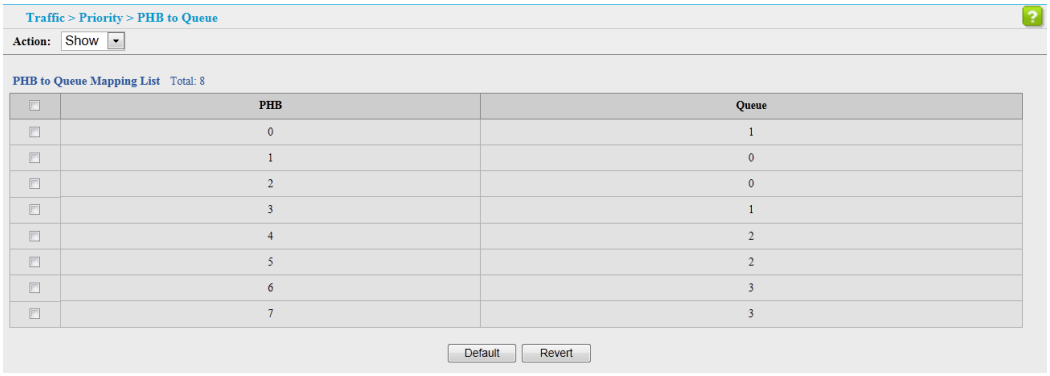


Table 8-10 Parameters of PHB to Queue

Title	Description
PHB	Per-hop behavior, or the priority used for this router hop. (Range: 0-7, where 7 is the highest priority)
Queue	Output queue. (Range: 0-3, where 3 is the highest CoS priority queue)

----End

8.4 Configuring Voice VLAN

When IP telephony is deployed in an enterprise network, it is recommended to isolate the Voice over IP (VoIP) network traffic from other data traffic. Traffic isolation can provide higher voice quality by preventing excessive packet delays, packet loss, and jitter. This is best achieved by assigning all VoIP traffic to a single Voice VLAN.

The use of a Voice VLAN has several advantages. It provides security by isolating the VoIP traffic from other data traffic. End-to-end QoS policies and high priority can be applied to VoIP VLAN traffic across the network, guaranteeing the bandwidth it needs. VLAN isolation also protects against disruptive broadcast and multicast traffic that can seriously affect voice quality.

The switch allows you to specify a Voice VLAN for the network and set a CoS priority for the VoIP traffic. The VoIP traffic can be detected on switch ports by using the source MAC address of packets. When VoIP traffic is detected on a configured port, the switch automatically assigns the port as a tagged member the Voice VLAN. Alternatively, switch ports can be manually configured.

8.4.1 Configuring Voice VLAN

Use the Traffic > Voice VLAN (Configure Global) page to configure the switch for VoIP traffic. First enable automatic detection of VoIP devices attached to the switch ports, then set the Voice VLAN ID for the network. The Voice VLAN aging time can also be set to remove a port from the Voice VLAN when VoIP traffic is no longer received on the port.

To configure global settings for a Voice VLAN:

1. Click Traffic, Voice VLAN.
2. Select Configure Global from the Step list.
3. Enable Auto Detection Status.
4. Specify the Voice VLAN ID.
5. Adjust the Voice VLAN Aging Time if required.
6. Click Apply.

Figure 8-14 Configuring a Voice VLAN

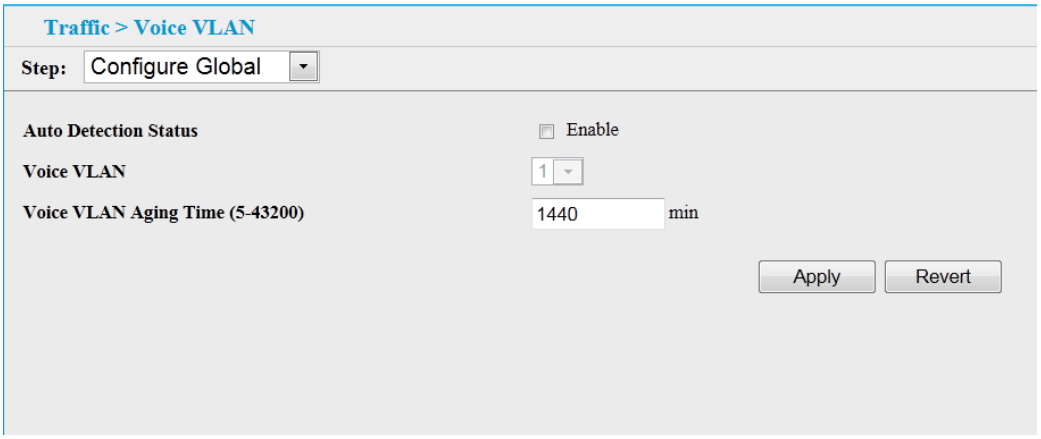


Table 8-11 Parameters of Configuring a Voice VLAN

Title	Description
Auto Detection Status	Enables the automatic detection of VoIP traffic on switch ports. (Default: Disabled)
Voice VLAN	Sets the Voice VLAN ID for the network. Only one Voice VLAN is supported and it must already be created on the switch. (Range: 1-4093)
Voice VLAN Aging Time	The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. (Range: 5-43200 minutes; Default: 1440 minutes)

CAUTION

- When auto detection enabled, users can modify Voice VLAN port.
- When the voice VLAN disabled, users can re-configure the configuration.

----End

8.4.2 Configuring Voice VLAN OUI

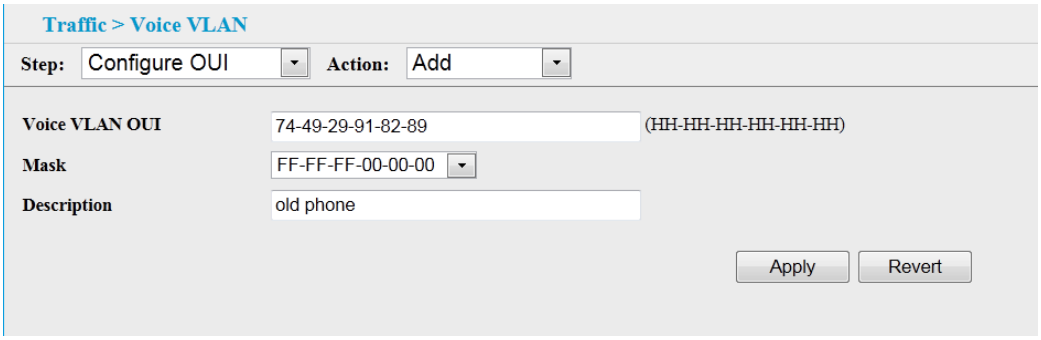
VoIP devices attached to the switch can be identified by the manufacturer's Organizational Unique Identifier (OUI) in the source MAC address of received packets. OUI numbers are assigned to manufacturers and form the first three octets of device MAC addresses. The MAC OUI numbers for VoIP equipment can be configured on the switch so that traffic from these devices is recognized as VoIP. Use the Traffic > Voice VLAN (Configure OUI) page to configure this feature.

To configure MAC OUI numbers for VoIP equipment:

1. Click Traffic, Voice VLAN.

2. Select Configure OUI from the Step list.
3. Select Add from the Action list.
4. Enter a MAC address that specifies the OUI for VoIP devices in the network.
5. Select a mask from the pull-down list to define a MAC address range.
6. Enter a description for the devices.
7. Click Apply.

Figure 8-15 Configuraing an OUI Telephony List



----End

To show/delete the MAC OUI numbers used for VoIP equipment:

1. Click Traffic, Voice VLAN.
2. Select Configure OUI from the Step list.
3. Select Show/delete from the Action list.

Figure 8-16 Showing/Deleting an OUI Telephony List

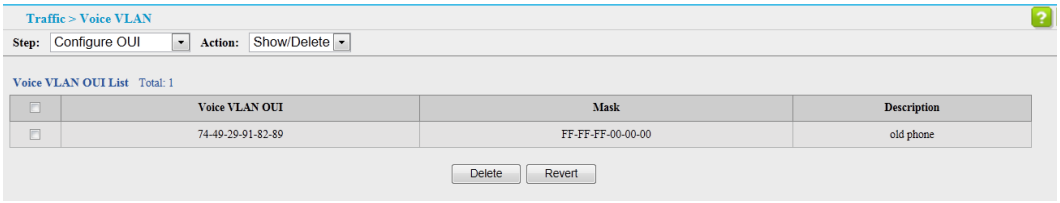


Table 8-12 Parameters of Configuring an OUI Telephony List

Title	Description
Telephony OUI	Specifies a MAC address range to add to the list. Enter the MAC address in format 01-23-45-67-89-AB.

Title	Description
Mask	Identifies a range of MAC addresses. Selecting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Selecting FF-FF-FF-FF-FF-FF specifies a single MAC address. (Default: FF-FF-FF-00-00-00)
Description	User-defined text that identifies the VoIP devices.

----End

8.4.3 Configuring VoIP Traffic Ports

Use the Traffic > Voice VLAN (Configure Interface) page to configure ports for VoIP traffic, you need to set the mode (Auto or Manual), specify the discovery method to use, and set the traffic priority. You can also enable security filtering to ensure that only VoIP traffic is forwarded on the Voice VLAN.

All ports are set to VLAN access mode by default. Prior to enabling VoIP for a port (by setting the VoIP mode to Auto or Manual as described below), first set the VLAN membership mode to hybrid.

To configure VoIP traffic settings for a port:

1. Click T raffic, Voice VLAN.
2. Select Configure Interface from the Step list.
3. Configure any required changes to the VoIP settings each port.
4. Click Apply.

Figure 8-17 Configuring Port Settings for a Voice VLAN

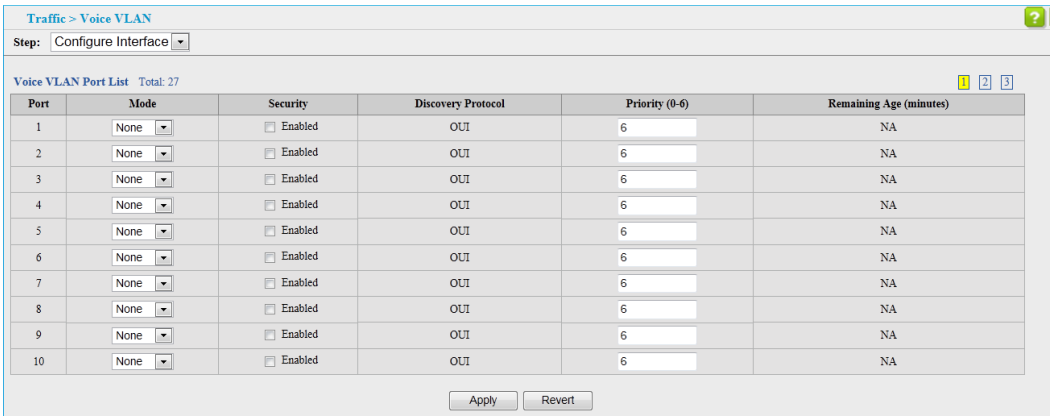


Table 8-13 Parameters of Configuring Port Settings for a Voice VLAN

Title	Description
Port	Specifies port id.
Mode	Specifies if the port will be added to the Voice VLAN when VoIP traffic is detected. (Default: None) • None – The Voice VLAN feature is disabled on the port. The port will not detect VoIP traffic or be added to the Voice VLAN. • Auto – The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port. When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list. • Manual – The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.
Security	Enables security filtering that discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list.
Discovery Protocol	OUI – Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address. OUI numbers are assigned to manufacturers and form the first three octets of a device MAC address. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.
Priority	Defines a CoS priority for port traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active for the port. (Range: 0-6; Default: 6)
Remaining Age	Number of minutes before this entry is aged out.

9 Security Measures

About This Chapter

9.1 AAA

The Authentication, authorization feature provides the main framework for configuring access control on the switch. The two security functions can be summarized as follows:

- Authentication — Identifies users that request access to the network.
- Authorization — Determines if users can access specific services.

To configure AAA on the switch, you need to follow this general process:

- Configure RADIUS server access parameters.
- Define RADIUS server to support the accounting and authorization of services.

CAUTION

This guide assumes that RADIUS servers have already been configured to support AAA. The configuration of RADIUS server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS server software.

9.1.1 Configuring Local/Remote Logon Authentication

Use the Security > AAA > System Authentication page to specify local or remote authentication. Local authentication restricts management access based on user names and passwords manually configured on the switch. Remote authentication uses a remote access authentication server based on RADIUS protocols to verify management access.

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence. Then specify the corresponding parameters for the remote authentication protocol using the Security > AAA > Server page. Local and remote logon authentication control management access via the web browser.
- You can specify up to four authentication methods for any user to indicate the authentication sequence. (1)Local, (2)RADIUS, (3) Local,RADIUS, (4) RADIUS, Local , For example, if you select (4), the user name and password is verified on the RADIUS server first. If the RADIUS server is not available, then authentication is attempted using the local user name and password is checked.

To configure the method(s) of controlling management access:

1. Click Security, AAA, System Authentication.
2. Specify the authentication sequence.
3. Click Apply.

Figure 9-1 Configuring the Authentication Sequence

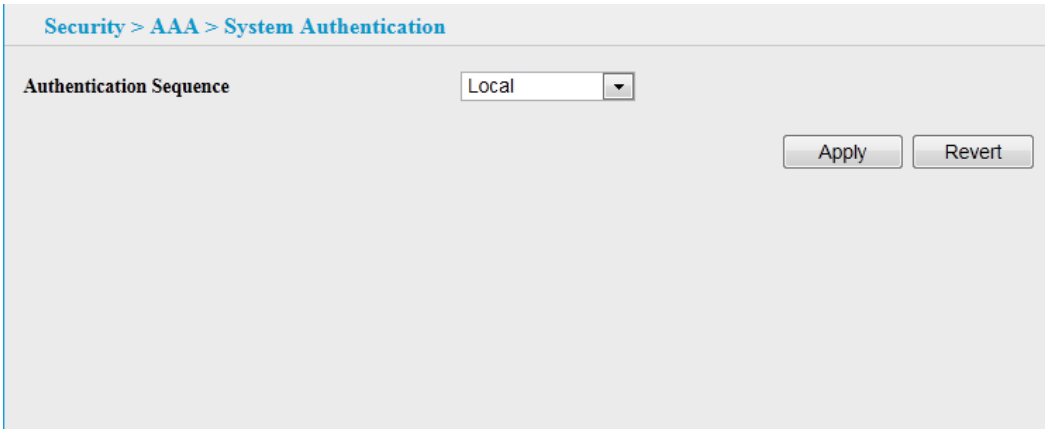


Table 9-1 Parameters of Configuring the Authentication Sequence

Title	Description
Authentication Sequence	Select the authentication, or authentication sequence required ,User authentication is performed by up to four authentication methods in the indicated sequence: • Local – User authentication is performed only locally by the switch. • RADIUS – User authentication is performed using a RADIUS server only. • Local, RADIUS – Priority for user authentication is performed locally by the switch. • RADIUS, Local – Priority for User authentication is performed using a RADIUS server

----End

9.1.2 Configuring Remote Logon Authentication Servers

Use the Security > AAA > Server page to configure the message exchange parameters for RADIUS remote access authentication servers.

Remote Authentication Dial-in User Service (RADIUS) is logon authentication protocols that use software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the switch.

- If a remote authentication server is used, you must specify the message exchange parameters for the remote authentication protocol. Both local and remote logon authentication control management access via the web browser.
- RADIUS logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server. The encryption methods used for the authentication process must also be configured or negotiated between the authentication server and logon client.

To configure the parameters for RADIUS authentication:

1. Click Security, AAA, Server.
2. To set or modify the authentication key, mark the Set Key box, enter the key, and then confirm it
3. Click Apply.

Figure 9-2 Configuring Remote Authentication Server

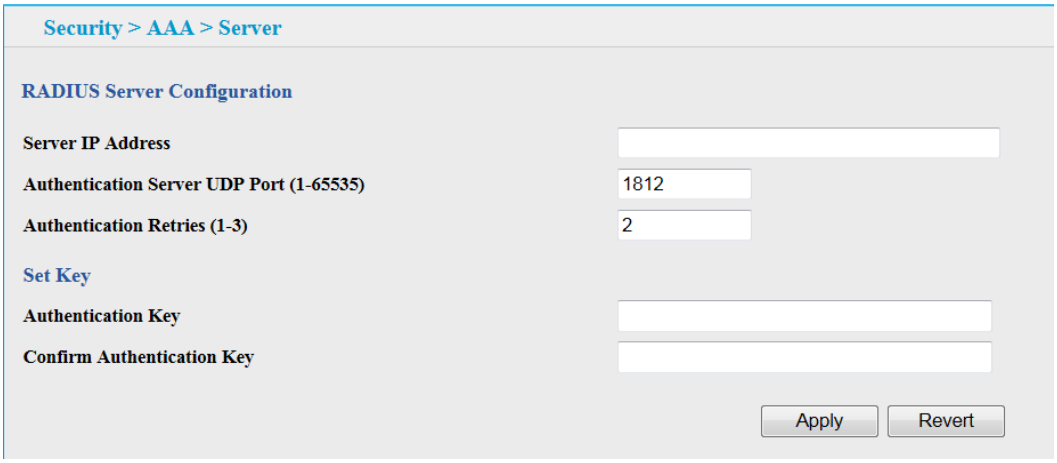


Table 9-2 Parameters of Configuring Remote Authentication Server

Title	Description
Server IP Address	Address of authentication server. (A Server Index entry must be selected to display this item.)
Authentication Server UDP Port	Network (UDP) port on authentication server used for authentication messages. (Range: 1-65535)
Authentication Retries	Number of times the switch tries to authenticate logon access via the authentication server. (Range: 1-3)
Set Key	Mark this box to set or modify the encryption key.
Authentication Key	Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)
Confirm Authentication Key	Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the encryption key if these two fields do not match.

----End

9.2 Configuring User Accounts

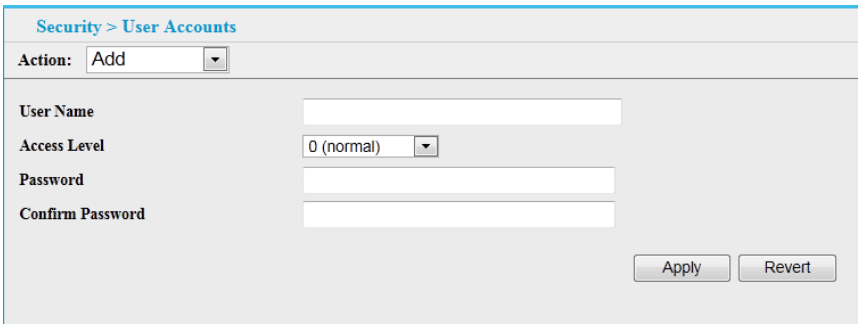
Use the Security > User Accounts page to control management access to the switch based on manually configured user names and passwords.

- The default administrator name is “admin” with the password “admin.”
- The normal user only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place.

To configure user accounts:

1. Click Security, User Accounts.
2. Select Add from the Action list.
3. Specify a user name, select the user's access level, then enter a password if required and confirm it.
4. Click Apply.

Figure 9-3 Configuring User Accounts

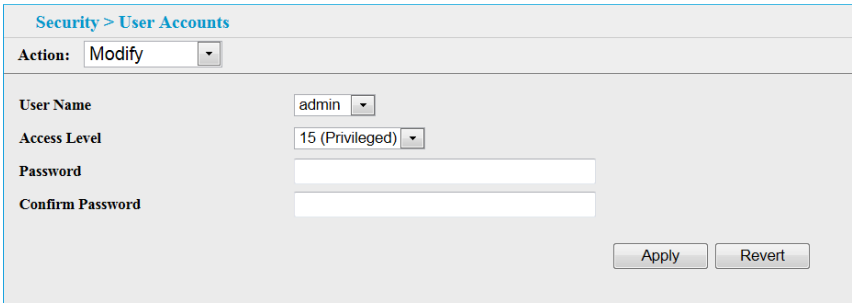


----End

To modify user accounts:

1. Click Security, User Accounts.
2. Select Modifyfrom the Action list.

Figure 9-4 Modifying User Accounts



----End

To show/delete user accounts:

1. Click Security, User Accounts.
2. Select Show/Delete from the Action list.

Figure 9-5 Showing/Deleting User Accounts

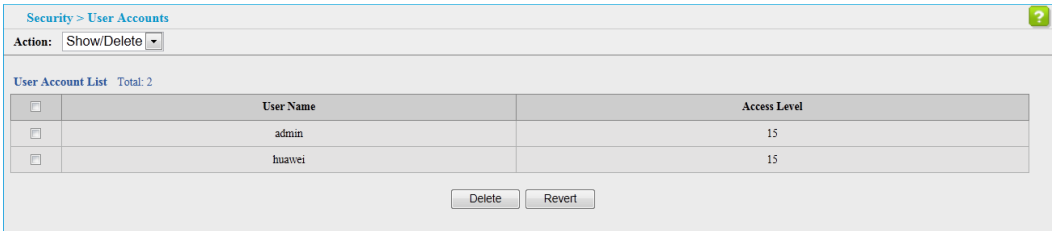


Table 9-3 Parameters of Configuring User Accounts

Title	Description
User Name	The name of the user. (Maximum length: 64 characters; maximum number of users: 16)
Access Level	Specifies the user level. (Options: 0 - Normal, 15 - Privileged) Normal privilege level provides access to a limited number of the commands which display the current status of the switch, as well as several database clear and reset functions. Privileged level provides full access to all commands.
Password	Password complexity requirements are as follows: (default password at least the detection complexity, meet the following requirements.) 1. Password length of at least 6 character password, maximum length of 16characters, can't set a password length; 2. Password must contain at least 2 of the following two kinds of combinations of characters: -At least one lowercase letters; -At least one uppercase letter; -At least one digital; -At least one special character; -Password special character list is as follows: ! $ % ( ) * + , - . / : ; < = > @ [\ ] ^ _ ` { | } ~ 3. Account or account password cannot be inverted to write the same; If you set the password does not meet the above rules, must carry warnings, then refused to accept, to require the user to input.
Confirm Password	Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the password if these two fields do not match.

----End

9.3 Network Access

Some devices connected to switch ports may not be able to support 802.1X authentication due to hardware or software limitations. This is often true for devices such as network printers, IP phones, and some wireless access points. The switch enables network access from these devices to be controlled by authenticating device MAC addresses with a central RADIUS server.

Displaying Secure MAC Address Information

Use the Security > Network Access page to display the authenticated MAC addresses stored in the secure MAC address table. Information on the secure

MAC entries can be displayed and selected entries can be removed from the table.

To display the authenticated MAC addresses stored in the secure MAC address table:

1. Security>network Access.
2. Use the sort key to display addresses based MAC address, interface, or attribute.
3. Restrict the displayed addresses by entering a specific address in the MAC Address field, specifying a port in the Interface field, or setting the address type to static or dynamic in the Attribute field.
4. Click Query.

Figure 9-6 Showing Addresses Authenticated for Network Access

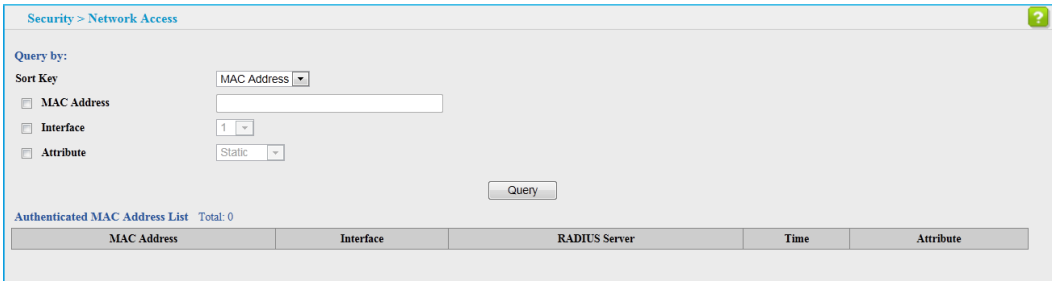


Table 9-4 Parameters of Showing Addresses Authenticatedd for Network Access

Title	Description
Query By	Specifies parameters to use in the MAC address query. • Sort Key – Sorts the information displayed based on MAC address, port interface, or attribute. • MAC Address – Specifies a specific MAC address. • Interface – Specifies a port interface. • Attribute – Displays static or dynamic addresses.

Title	Description
Authenticated MAC Address List	• MAC Address – The authenticated MAC address. • Interface – The port interface associated with a secure MAC address. • RADIUS Server – The IP address of the RADIUS server that authenticated the MAC address. • Time – The time when the MAC address was last authenticated. • Attribute – Indicates a static or dynamic address.

----End

9.4 Filtering IP Addresses for Management Access

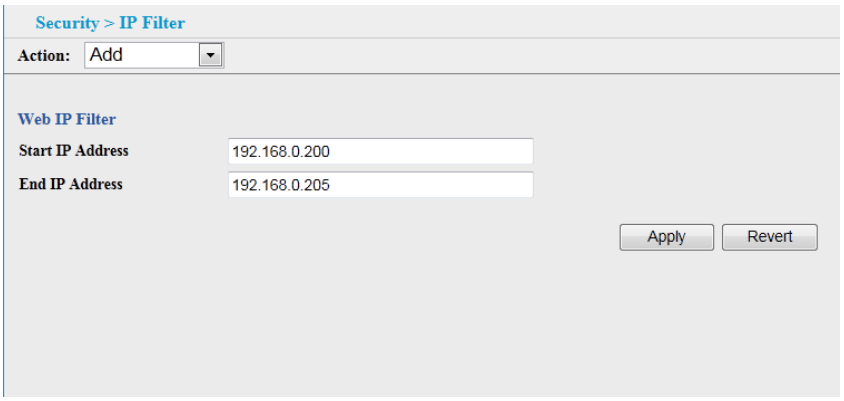
Use the Security > IP Filter page to create a list of up to 5 IP addresses or IP address groups that are allowed management access to the switch through the web interface.

9.4.1 Creating a list of IP addresses authorized

To create a list of IP addresses authorized for management access:

1. Click Security, IP Filter.
2. Select Add from the Action list.
3. Enter the IP addresses or range of addresses that are allowed management access to an interface.
4. Click Apply

Figure 9-7 Creating an IP Address Filter for Management Access



----End

9.4.2 Showing/deleting a list of IP addresses authorized

To show/delete a list of IP addresses authorized for management access:

1. Click Security, IP Filter.
2. Select Show/Delete from the Action list.

Figure 9-8 Showing/Deleting Configured IP Address Filter for Management Access

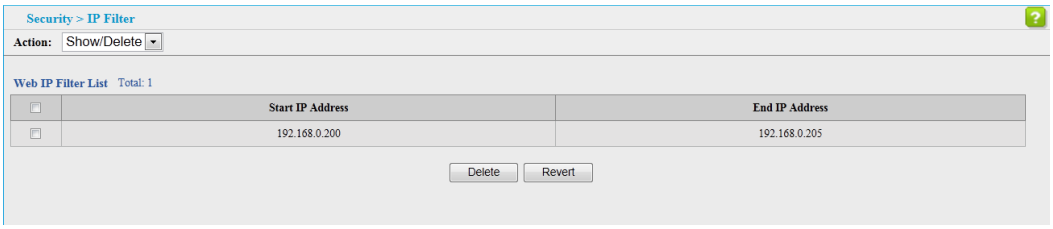


Table 9-5 Parameters of Creating an IP Address Filter for Management Access

Title	Description
Start IP Address	A single IP address, or the starting address of a range.
End IP Address	The end address of a range.

----End

9.5 Configuring Port Isolation

Use the Security > Port Isolation page to enable or disable the port isolation function on the specified port/trunk.

To configure port isolation:

1. Click Security, Port Isolation.
2. Select Port or Trunk as the Interface.
3. Select Enable or not for the specified port/trunk
4. Click Apply.

Figure 9-9 Configuring Port Isolation

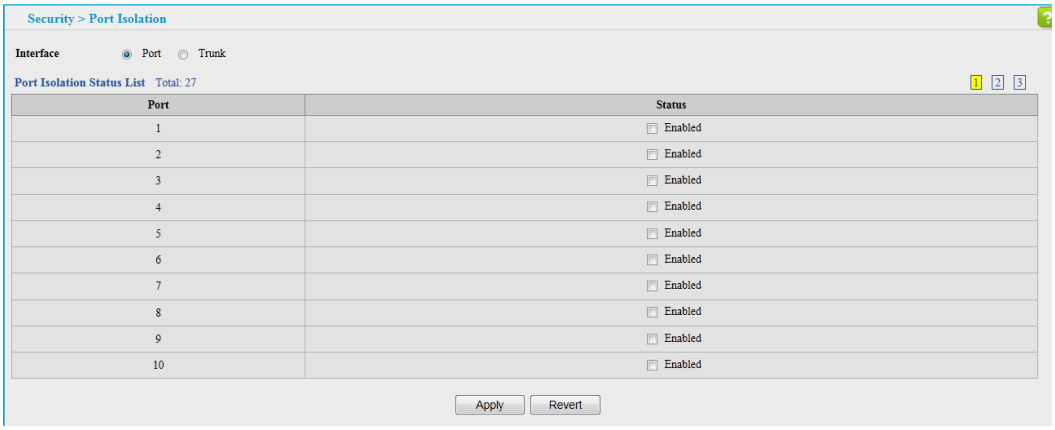


Table 9-6 Parameters of Configuring Port Isolation

Title	Description
Port	Port number.
Status	Enables or disables port isolation on the port.(Default: Disabled)

----End

9.6 Configuring 802.1x Port Authentication

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1X (dot1X) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The encryption method used to pass authentication messages can be MD5 (Message-Digest 5), TLS (Transport Layer Security), PEAP (Protected Extensible Authentication Protocol), or TTLS (Tunneled Transport Layer Security). The client

responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, non-EAP traffic on the port is blocked or assigned to a guest VLAN based on the "intrusion-action" setting. In "multi-host" mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for allhosts if one attached host fails re-authentication or sends an EAPOL logoff message.

9.6.1 Configuring 802.1x Global Settings

Use the Security > Port Authentication (Configure Global) page to configure IEEE 802.1X port authentication. The 802.1X protocol must be enabled globally for the switch system before port settings are active.

To configure global settings for 802.1X:

1. Click Security, Port Authentication.
2. Select Configure Global from the Step list.
3. Enable 802.1X globally for the switch.
4. Click Apply

Figure 9-10 Configuring Global Settings for 802.1x Port Authentication

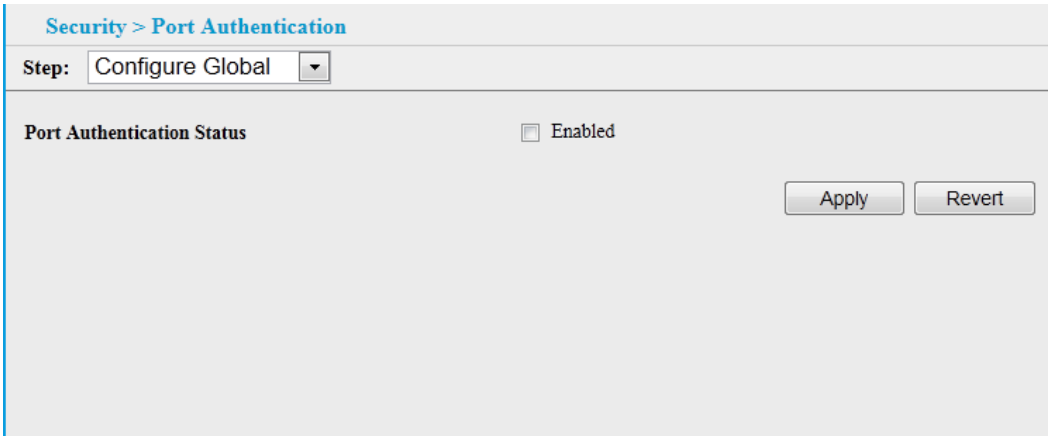


Table 9-7 Parameters of Configuring Global Settings for 802.1x Port Authentication

Title	Description
Port Authentication Status	Sets the global setting for 802.1X. (Default: Disabled)

----End

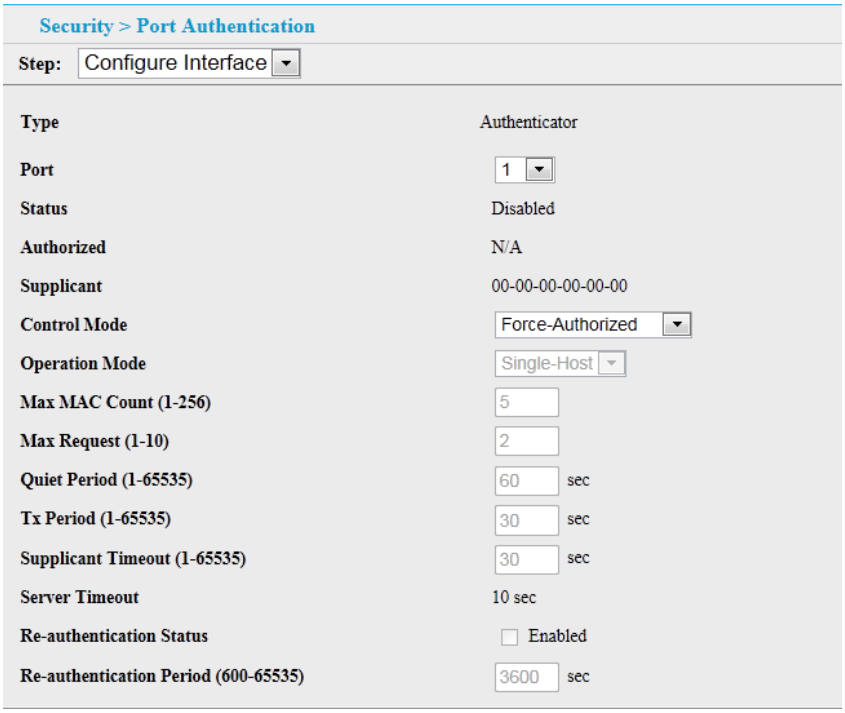
9.6.2 Configuring Port Authentication Settings for 802.1x

Use the Security > Port Authentication (Configure Interface) page to configure 802.1X port settings for the switch as the local authenticator. When 802.1X is enabled, you need to configure the parameters for the authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server.

To configure port authenticator settings for 802.1X:

1. Click Security, Port Authentication.
2. Select Configure Interface from the Step list.
3. Modify the authentication settings for each port as required.
4. Click Apply.

Figure 9-11 Configuring Interface Settings for 802.1x Port Authentication



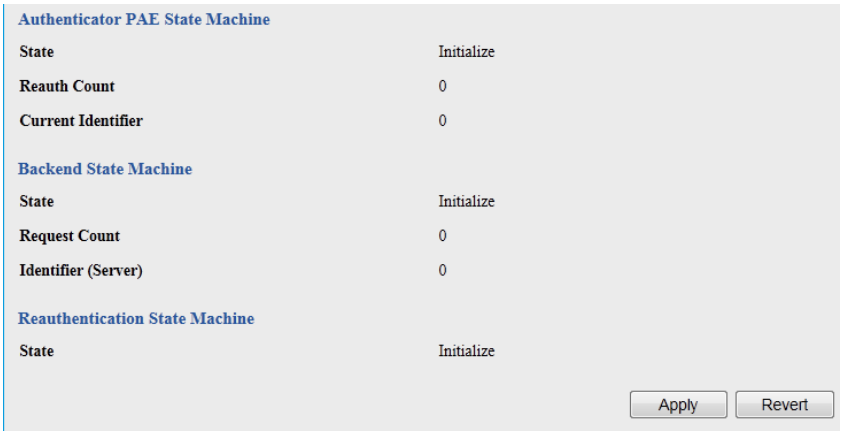


Table 9-8 Parameters of Configuring Interface Settings for 802.1X Port Authentication

Title	Description
Port	Port number.
Status	Indicates if authentication is enabled or disabled on the port. The status is disabled if the control mode is set to Force-Authorized.
Authorized	Displays the 802.1X authorization status of connected clients. • Yes – Connected client is authorized. • No – Connected client is not authorized.
Supplicant	Indicates the MAC address of a connected client.
Control Mode	Sets the authentication mode to one of the following options: • Auto – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access. • Force-Authorized – Forces the port to grant access to all clients, either dot1x-aware or otherwise. (This is the default setting.) • Force-Unauthorized – Forces the port to deny access to all clients, either dot1x-aware or otherwise.
Operation Mode	Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. (Default: Single-Host) • Single-Host – Allows only a single host to connect to this port. • Multi-Host – Allows multiple host to connect to this port. In this mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.
Max MAC Count	The maximum number of hosts that can connect to a port when the Multi-Host operation mode is selected.(Range: 1-256; Default: 5)

Title	Description
Max-Request	Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)
Quiet Period	Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)
Tx Period	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)
Supplicant Timeout	Sets the time that a switch port waits for a response to an EAP request from a client before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)
Server Timeout	Sets the time that a switch port waits for a response to an EAP request from an authentication server before re-transmitting an EAP packet.
Re-authentication Status	Sets the client to be re-authenticated after the interval specified by the Re-authentication Period. Reauthentication can be used to detect if a new device is plugged into a switch port. (Default: Disabled)
Re-authentication Period	Sets the time period after which a connected client must be re-authenticated. (Range: 600-65535 seconds; Default: 3600 seconds)
Authenticator PAE State Machine	
State	Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
Reauth Count	Number of times connecting state is re-entered.
Current Identifier	Identifier sent in each EAP Success, Failure or Request packet by the Authentication Server.
Backend State Machine	
State	Current state (including request, response, success, fail, timeout, idle, initialize).
Request Count	Number of EAP Request packets sent to the Supplicant without receiving a response.
Identifier (Server)	Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.
Reauthentication State Machine	
State	Current state (including initialize, reauthenticate).

----End

9.6.3 Displaying 802.1x Statistics

Use the Security > Port Authentication (Show Statistics) page to display statistics for dot1x protocol exchanges for any port.

To display port authenticator statistics for 802.1X:

1. Click Security, Port Authentication.
2. Select Show Statistics from the Step list.
3. Select port.

Figure 9-12 Showing Statistics for 802.1x Port Authentication

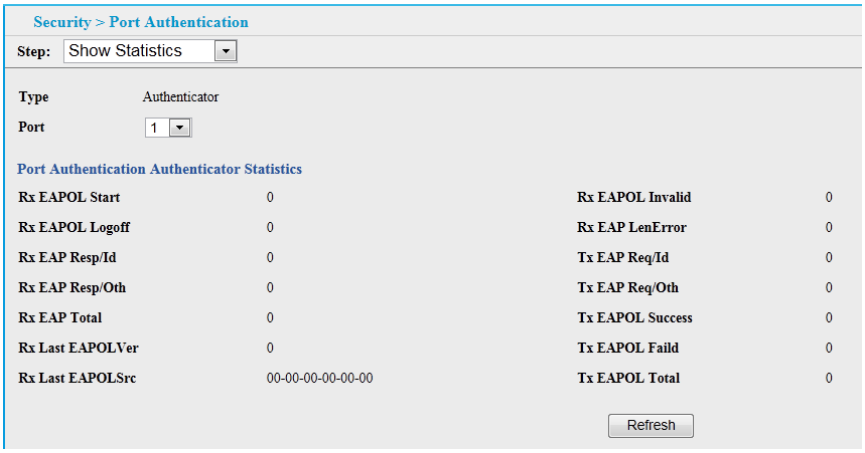


Table 9-9 Parameters of Statistics for 802.1x Port Authentication

Title	Description
Rx EAPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx Last EAPOLVer	The protocol version number carried in the most recent EAPOL frame received by this Authenticator.
Rx Last EAPOLSrc	The source MAC address carried in the most recent EAPOL frame received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.

Title	Description
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/ Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
Tx EAP Success	The number of EAPOL frames of any type that have been transmitted success by this Authenticator.
Tx EAP Failed	The number of EAPOL frames of any type that have been transmitted failed by this Authenticator.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.

----End

10 Management

About This Chapter

10.1 Configuring Event Logging

The switch allows you to control the logging of error messages, including the type of events that are recorded in switch memory, logging to a remote System Log (syslog) server, and displays a list of recent event messages.

10.1.1 System Log Configuration

Use the Administration > Log > System (Configure Global) page to enable or disable event logging, and specify which levels are logged to RAM or flash memory.

The switch can store up to 2048 log entries in temporary random access memory (RAM; i.e., memory flushed on power reset) and up to 512 entries in permanent flash memory.

The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

To configure the logging of error messages to system memory:

1. Click Administration, Log, System.
2. Select Configure Global from the Step list.
3. Enable or disable system logging, set the level of event messages to be logged to flash memory and RAM.
4. Click Apply.

Figure 10-1 Configuring Settings for System Memory Logs

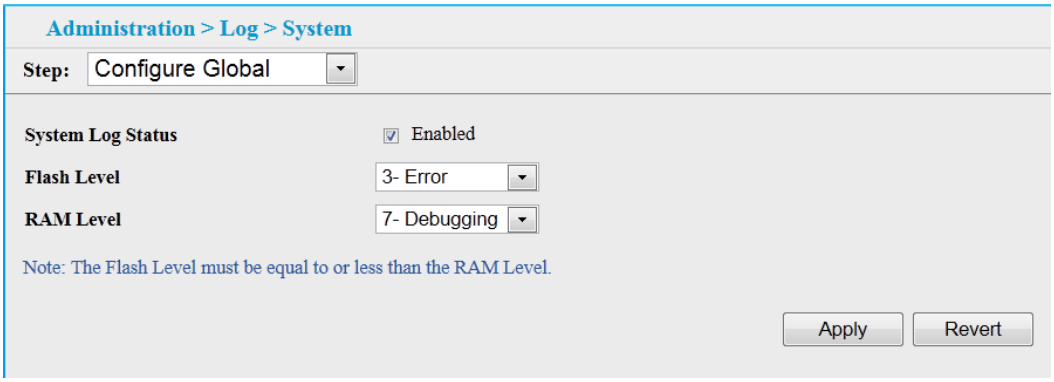


Table 10-1 Parameters of Configuring Settings for System Memory Logs

Title	Description
System Log Status	Enables/disables the logging of debug or error messages to the logging process. (Default: enable)
Flash Level	Limits log messages saved to the switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. (Range: 0-7, Default: 3) Detailed Logging Level description, please see Table 10-2.
RAM Level	Limits log messages saved to the switch's temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM. (Range: 0-7, Default: 7) Detailed Logging Level description, please see Table 10-2.

Table 10-2 Logging Levels

Level	Severity Name	Descriptin
7	Debugging	Debugging messages
6	Informational	Informational messages only
5	Notice	Normal but significant condition, such as cold start
4	Warning	Warning conditions (e.g., return false, unexpected return)
3	Error	Error conditions (e.g., invalid input, default used)
2	Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	Alert	Immediate action needed
0	Emergency	System unusable

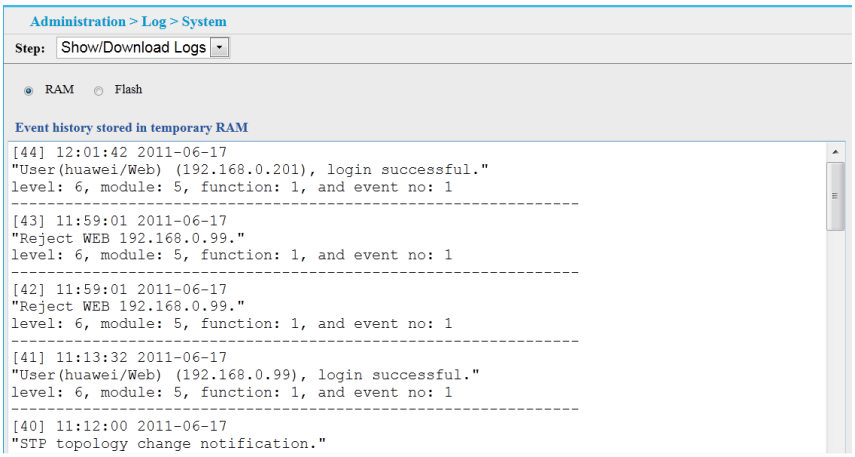
----End

10.1.2 Show/download log

To show the error messages logged to system or flash memory:

1. Click Administration, Log, System.
2. Select Show Logs from the Step list.
3. Click RAM to display log messages stored in system memory, or Flash to display messages stored in flash memory.

Figure 10-2 Showing Error Messages Logged to System Memory



----End

10.1.3 Remote Log Configuration

Use the Administration > Log > Remote page to send log messages to syslog servers or other management stations. You can also limit the event messages sent to only those messages below a specified level.

To configure the logging of error messages to remote servers:

1. Click Administration, Log, Remote.
2. Enable remote logging, specify the facility type to use for the syslog messages. and enter the IP address of the remote servers.
3. Click Apply.

Figure 10-3 Configuring Settings for Remote Logging of Error Message

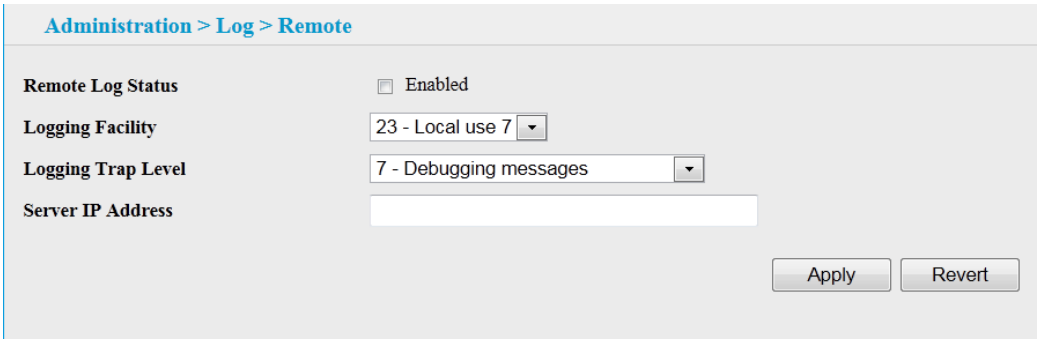


Table 10-3 Parameters of Configuring Settings for Remote Logging of Error Message

Title	Description
Remote Log Status	Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)
Logging Facility	Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service. The attribute specifies the facility type tag sent in syslog messages (see RFC 3164). This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)
Logging Trap Level	Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Range: 0-7, Default: 7)
Server IP Address	Specifies the IP address of a remote server which will be sent syslog messages.

----End

10.2 Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

10.2.1 Setting LLDP Timing Attributes

Use the Administration > LLDP (Configure Global) page to set attributes for general functions such as globally enabling LLDP on the switch, setting the message ageout time, and setting the frequency for broadcasting general advertisements.

To configure LLDP timing attributes:

1. Click Administration, LLDP.
2. Select Configure Global from the Step list.
3. Enable LLDP, and modify any of the timing parameters as required.
4. Click Apply.

Figure 10-4 Configuring LLDP Timing Attributes

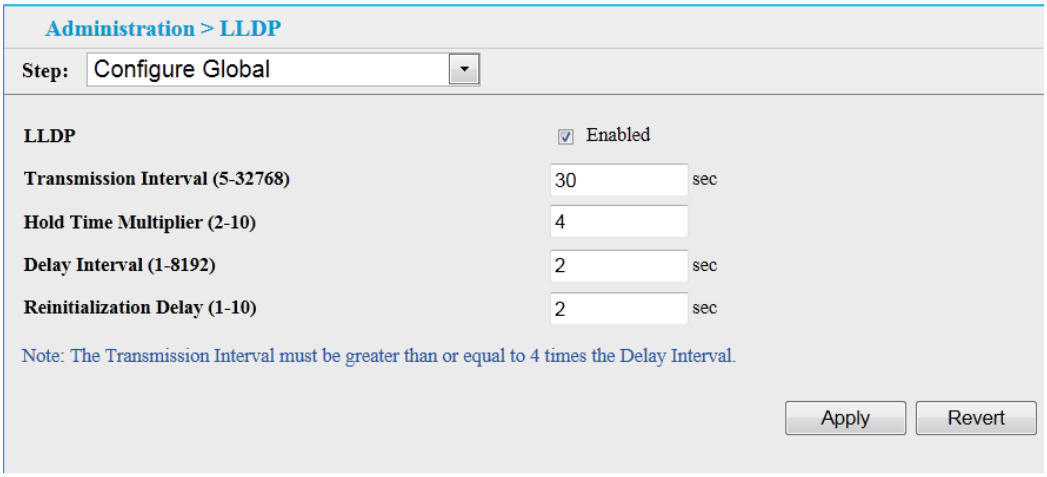


Table 10-4 Parameters of Configuring LLDP Timing Attributes

Title	Description
LLDP	Enables LLDP globally on the switch. (Default: Enabled)
Transmission Interval	Configures the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds) This attribute must comply with the following rule: (Transmission Interval >= (4 * Delay Interval)
Hold Time Multiplier	Configures the time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4) The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner. TTL in seconds is based on the following rule: (The default TTL is 4*30 = 120 seconds.

Title	Description
Delay Interval	Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. (Range: 1-8192 seconds; Default: 2 seconds) The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission. This attribute must comply with the rule: (4 * Delay Interval) ≤ Transmission Interval
Reinitialization Delay	Configures the delay before attempting to reinitialize after LLDP ports are disabled or the link goes down. (Range: 1-10 seconds; Default: 2 seconds) When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

----End

10.2.2 Configuring LLDP Interface Attributes

Use the Administration > LLDP page to specify the message attributes for individual interfaces, including whether messages are transmitted, received, or both transmitted and received, and the type of information advertised.

To configure LLDP interface attributes:

1. Click Administration, LLDP.
2. Select Configure Interface from the Step list.
3. Select an interface from the Port or Trunk list.
4. Set the LLDP transmit/receive mode, and select the information to advertise in LLDP messages.
5. Click Apply.

Figure 10-5 Configuring LLDP Interface Attributes

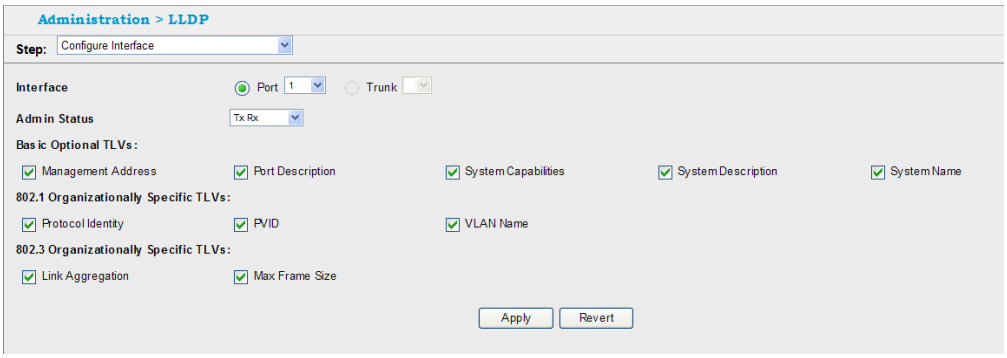


Table 10-5 Parameters of Configuring LLDP Interface Attributes

Title	Description
Admin Status	Enables LLDP message transmit and receive modes for LLDP Protocol Data Units. (Options: Tx only, Rx only, TxRx, Disabled; Default: TxRx)
Basic Optional TLVs	Configures basic information included in the TLV field of advertised messages. • Management Address – The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement. The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications in the performance of network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB. Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV. Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV. • Port Description – The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software. • System Capabilities – The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB. • System Description – The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software. • System Name – The system name is taken from the sysName object in RFC 3418, which contains the system’s administratively assigned name. To configure the system name.

Title	Description
802.1 Organizationally Specific TLVs	Configures IEEE 802.1 information included in the TLV field of advertised messages. • Protocol Identity – The protocols that are accessible through this interface. • VLAN ID – The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated. • VLAN Name – The name of all VLANs to which this interface has been assigned. • Port and Protocol VLAN ID – The port-based protocol VLANs configured on this interface
802.3 Organizationally Specific TLVs	Configures IEEE 802.3 information included in the TLV field of advertised messages. • Link Aggregation – The link aggregation capabilities, aggregation status of the link, and the IEEE 802.3 aggregated port identifier if this interface is currently a link aggregation member. • Max Frame Size – The maximum frame size.

----End

10.2.3 Displaying LLDP Local Device Information

Use the Administration > LLDP (Show Local Device Information) page to display information about the switch, such as its Chassic type, Chassis ID, System Name, System Description, System Capabilities Supported , System Capabilities Enabled , Management Address.

To display LLDP information for the local device:

1. Click Administration, LLDP.
2. Select Show Local Device Information from the Step list.
3. Select General, Port, or Trunk.

Figure 10-6 Displaying Local Device Information for LLDP-General.

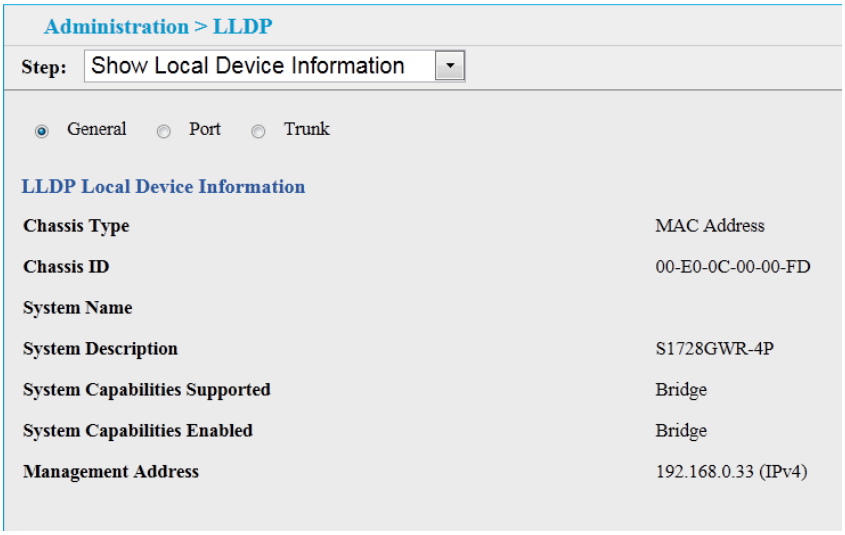
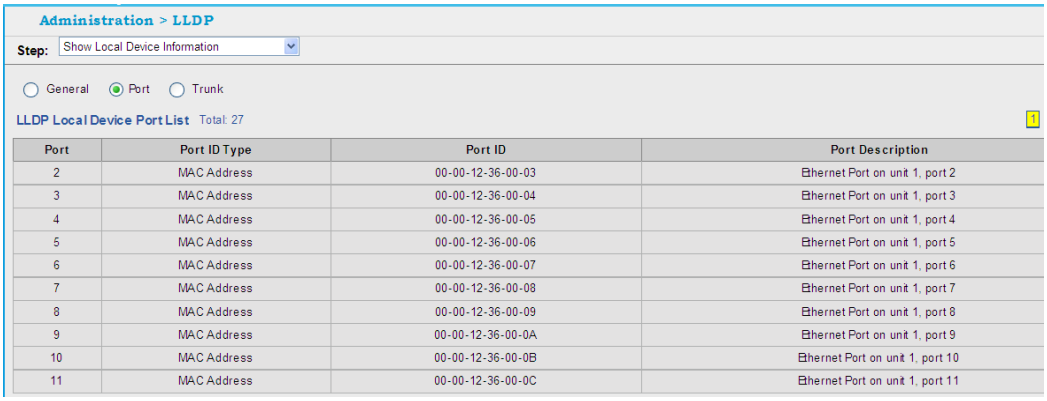


Table 10-6 Parameters of Displaying Local Device Information for LLDP-General.

Title	Description
Chassis Type	Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.
Chassis ID	An octet string indicating the specific identifier for the particular chassis in this system.
System Name	A string that indicates the system's administratively assigned name.
System Description	A textual description of the network entity. This field is also displayed by the show system command.
System Capabilities Supported	The capabilities that define the primary function(s) of the system as.
System Capabilities Enabled	The primary function(s) of the system which are currently enabled. Refer to the preceding table.
Management Address	The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

Figure 10-7 Displaying Local Device Information for LLDP-Port.

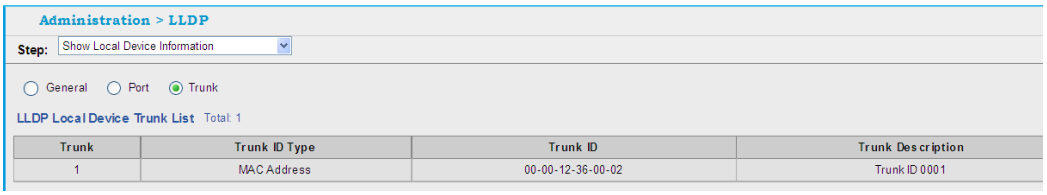


Port	Port ID Type	Port ID	Port Description
2	MAC Address	00-00-12-36-00-03	Ethernet Port on unit 1, port 2
3	MAC Address	00-00-12-36-00-04	Ethernet Port on unit 1, port 3
4	MAC Address	00-00-12-36-00-05	Ethernet Port on unit 1, port 4
5	MAC Address	00-00-12-36-00-06	Ethernet Port on unit 1, port 5
6	MAC Address	00-00-12-36-00-07	Ethernet Port on unit 1, port 6
7	MAC Address	00-00-12-36-00-08	Ethernet Port on unit 1, port 7
8	MAC Address	00-00-12-36-00-09	Ethernet Port on unit 1, port 8
9	MAC Address	00-00-12-36-00-0A	Ethernet Port on unit 1, port 9
10	MAC Address	00-00-12-36-00-0B	Ethernet Port on unit 1, port 10
11	MAC Address	00-00-12-36-00-0C	Ethernet Port on unit 1, port 11

Table 10-7 Parameters of Displaying Local Device Information for LLDP-port

Title	Description
Port	Port.
Port ID Type	The type of Port ID.
Port ID	A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
Port Description	A string that indicates the port description. If RFC 2863 is implemented, the ifDescr object should be used for this field.

Figure 10-8 Displaying Local Device Information for LLDP-Truck.



Trunk	Trunk ID Type	Trunk ID	Trunk Description
1	MAC Address	00-00-12-36-00-02	Trunk ID 0001

Table 10-8 Parameters of Displaying Local Device Information for LLDP- truck.

Title	Description
Trunk	Trunk.
Trunk ID Type	The type of Trunk ID.
Trunk ID	A string that contains the specific identifier for the trunk from which this LLDPDU was transmitted.
Trunk Description	A string that indicates the trunk description. If RFC 2863 is implemented, the ifDescr object should be used for this field.

----End

10.2.4 Displaying LLDP Remote Port Information

Use the Administration > LLDP (Show Remote Device Information) page to display information about devices connected directly to the switch's ports which are advertising information through LLDP, or to display detailed information about an LLDP-enabled device connected to a specific port on the local switch.

To display LLDP information for a remote port:

1. Click Administration, LLDP.
2. Select Show Remote Device Information from the Step list.
3. Select Port, Port Details, Trunk, or Trunk Details.

Figure 10-9 Displaying Remote Device Information for LLDP-Port

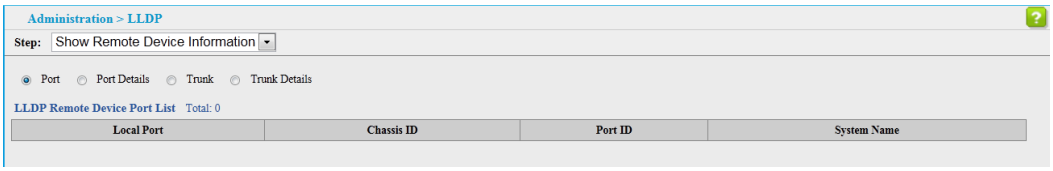


Table 10-9 Parameters of Displaying Remote Device Information for LLDP-Port

Title	Description
Local Port	The local port to which a remote LLDP-capable device is attached.
Chassis ID	An octet string indicating the specific identifier for the particular chassis in this system.
Port ID	A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
System Name	A string that indicates the system's administratively assigned name.

Figure 10-10 Displaying Remote Device Information for LLDP-Port Details

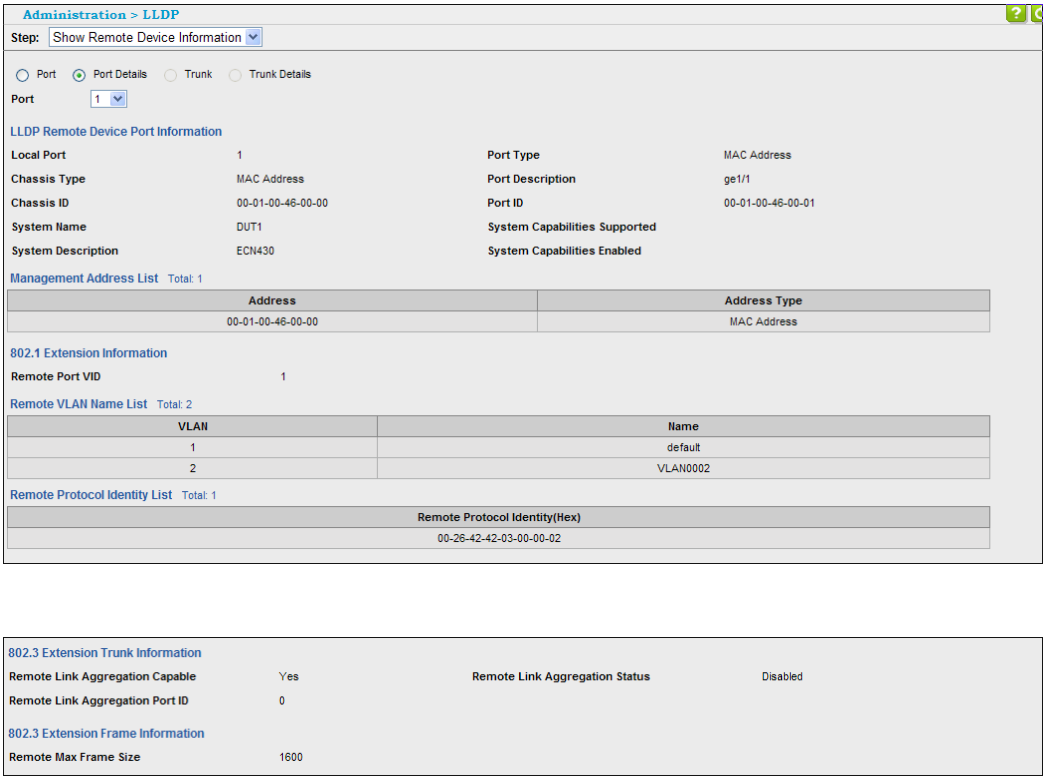


Table 10-10 Parameters of Displaying Remote Device Information for LLDP-Port Details

Title	Description
Local Port	The local port to which a remote LLDP-capable device is attached.
Chassis Type	Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.
Chassis ID	An octet string indicating the specific identifier for the particular chassis in this system.
System Name	A string that indicates the system's administratively assigned name.
System Description	A textual description of the network entity.
Port Type	Indicates the basis for the identifier that is listed in the Port ID field.
Port Description	A string that indicates the port's description. If RFC 2863 is implemented, the ifDescr object should be used for this field.

Title	Description
Port ID	A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
System Capabilities Supported	The capabilities that define the primary function(s) of the system.
System Capabilities Enabled	The primary function(s) of the system which are currently enabled.
Management Address	The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.
802.1 Extension Information	Display IEEE 802.1 Extension Information associated with the remote port.
Remote Port VID	Identify the port's VLAN identifier associated with the remote port.
Remote VLAN Name List	Display all VLAN Names associated with the remote port.
Remote Protocol Identity List	Display all Protocol Identities associated with the remote system.
802.3 Extension Trunk information	Display IEEE 802.3 Extension Trunk information associated with the remote port.
802.3 Extension Frame information	Display IEEE 802.3 Extension Frame information associated with the remote port.

Figure 10-11 Displaying Remote Device Information for LLDP-Truck

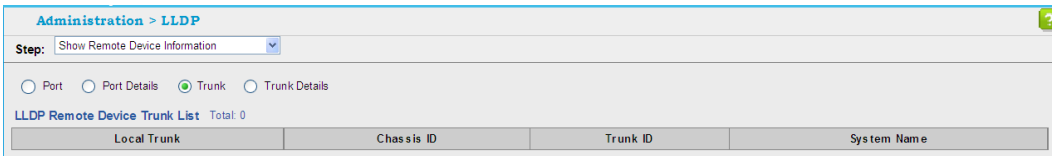


Table 10-11 Parameters of Displaying Remote Device Information for LLDP-Truck

Title	Description
Local Trunk	The local Trunk to which a remote LLDP-capable device is attached.
Chassis ID	An octet string indicating the specific identifier for the particular chassis in this system.
Trunk ID	A string that contains the specific identifier for the Trunk from which this LLDPDU was transmi

Title	Description
System Name	A string that indicates the system‘s administratively assigned name.

Figure 10-12 Displaying Remote Device Information for LLDP-Truck Details

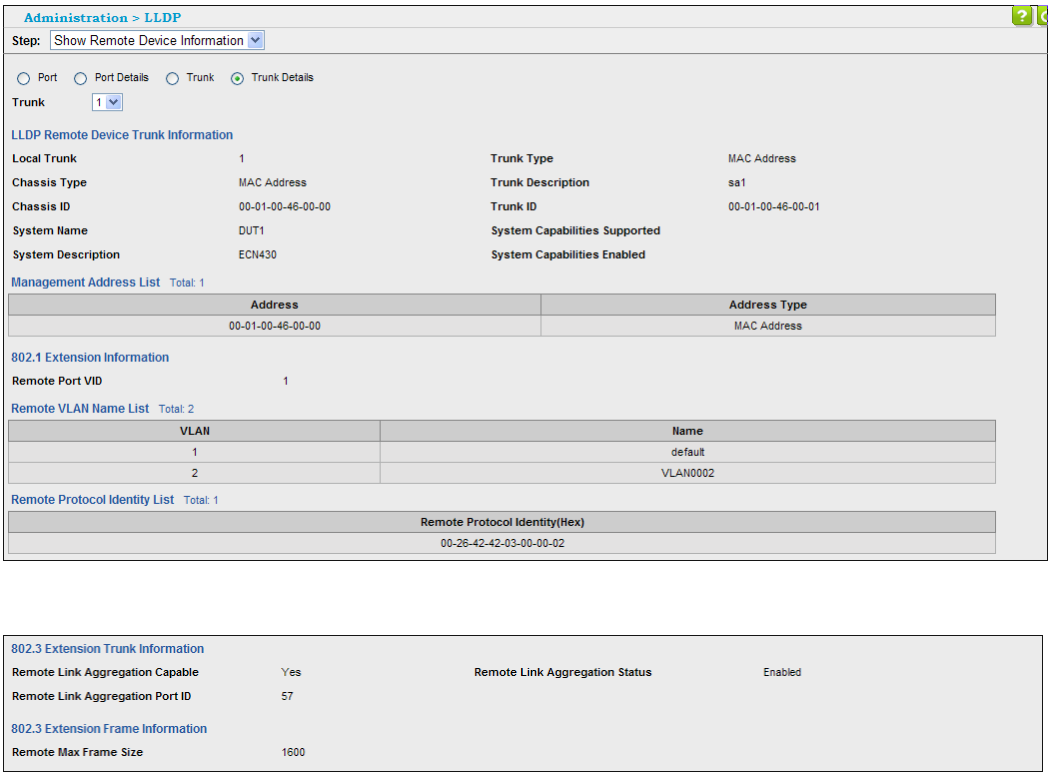


Table 10-12 Parameters of Displaying Remote Device Information for LLDP-Truck Details

Title	Description
Local Trunk	The local Trunk to which a remote LLDP-capable device is attached.
Chassis Type	Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.
Chassis ID	An octet string indicating the specific identifier for the particular chassis in this system.
System Name	A string that indicates the system‘s administratively assigned name.
System Description	A textual description of the network entity.

Title	Description
Trunk Type	The type of Trunk.
Trunk Description	A string that indicates the Trunk‘s description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
Trunk ID	A string that contains the specific identifier for the Trunk from which this LLDPDU was transm
System Capabilities Supported	The capabilities that define the primary function(s) of the system.
System Capabilities Enabled	The primary function(s) of the system which are currently enabled.
Management Address	The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.
802.1 Extension Information	Display IEEE 802.1 Extension Information associated with the remote trunk.
Remote Port VID	Identify the trunk's VLAN identifier associated with the remote trunk.
Remote VLAN Name List	Display all VLAN Names associated with the remote trunk.
Remote Protocol Identity List	Display all Protocol Identities associated with the remote system.
802.3 Extension trunk Information	Display IEEE 802.3 Extension Trunk Information associated with the remote trunk.
802.3 Extension Frame Information	Display IEEE 802.3 Extension Frame Information associated with the remote trunk.

----End

10.2.5 Displaying Device Statistics

Use the Administration > LLDP (Show Device Statistics) page to display statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces.

To display statistics for LLDP-capable devices attached to the switch:

1. Click Administration, LLDP.
2. Select Show Device Statistics from the Step list.
3. Select General, Port, or Trunk.

Figure 10-13 Displaying LLDP Device Statistics (General)

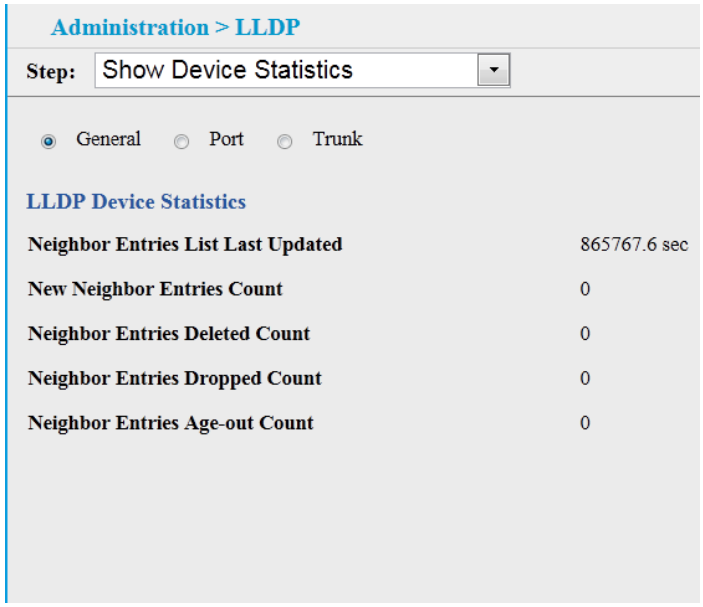


Table 10-13 Parameters of Displaying LLDP Device Statistics (General)

Title	Description
Neighbor Entries List Last Updated	The time the LLDP neighbor entry list was last updated.
New Neighbor Entries Count	The number of LLDP neighbors for which the remote TTL has not yet expired.
Neighbor Entries Deleted Count	The number of LLDP neighbors which have been removed from the LLDP remote systems MIB for any reason.
Neighbor Entries Dropped Count	The number of times which the remote database on this switch dropped an LLDPDU because of insufficient resources.
Neighbor Entries Age-out Count	The number of times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

Figure 10-14 Displaying LLDP Device Statistics (Port)

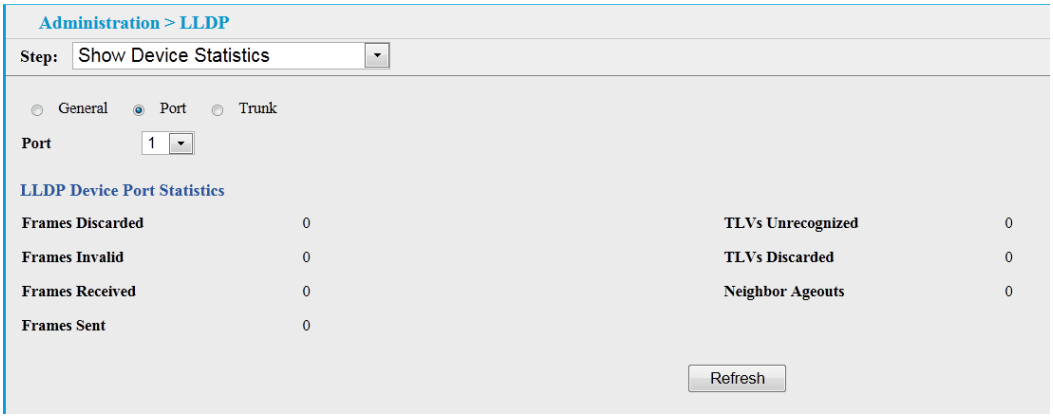


Figure 10-15 Displaying LLDP Device Statistics (Truck)

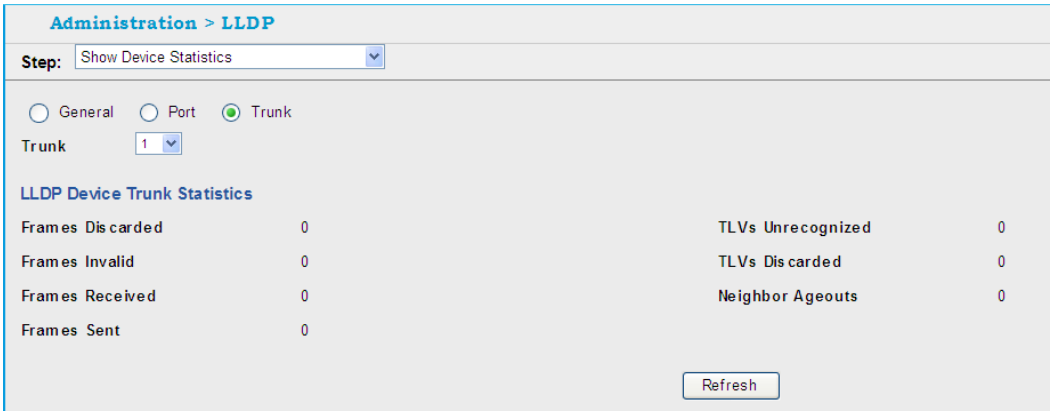


Table 10-14 Parameters of Displaying LLDP Device Statistics (Port/Trunk)

Title	Description
Frames Discarded	Number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular TLV.
Frames Invalid	A count of all LLDPDUs received with one or more detectable errors.
Frames Received	Number of LLDP PDUs received.
Frames Sent	Number of LLDP PDUs transmitted.
TLVs Unrecognized	A count of all TLVs not recognized by the receiving LLDP local agent.
TLVs Discarded	A count of all LLDPDUs received and then discarded due to insufficient memory space, missing or out-of-sequence attributes, or any other reason.

Title	Description
Neighbor Ageouts	A count of the times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

----End

11 IP Configuration

About This Chapter

This chapter provides information on network functions including:

11.1 Using the PING Function

Use the IP > General > Ping page to send ICMP echo request packets to another node on the network.

To ping another device on the network:

1. Click IP, General, Ping.
2. Specify the target device and ping parameters.
3. Click Apply.

Figure 11-1 Pinging a Network Device

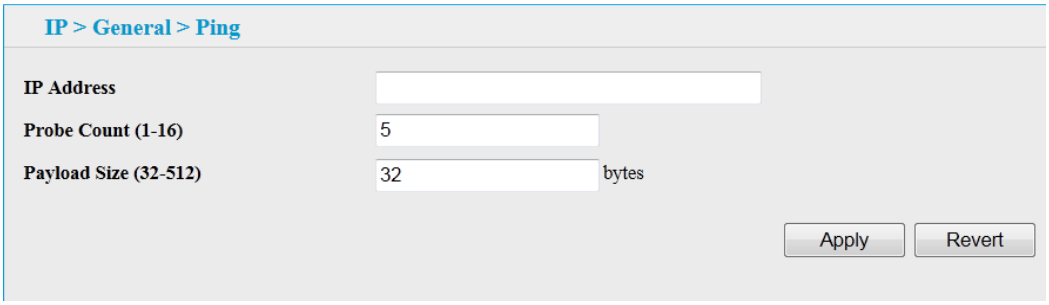


Table 11-1 Parameters of Ping

Title	Description
IP Address	IP address of the host.
Probe Count	Number of packets to send. (Range: 1-16, default: 5)
Payload Size	Number of bytes in a packet. (Range: 32-512 bytes, default: 32)

----End

11.2 Address Resolution Protocol

Address Resolution Protocol (ARP) is used to map an IP address to a physical layer address. When a device sends or receives a packet with an IP header, it must first resolve the destination IP address into a MAC address. When an IP frame is received by this switch, it first looks up the MAC address corresponding to the destination IP address in the ARP cache. If the address is found, the switch writes the MAC address into the appropriate field in the frame header, and forwards the frame on to the destination.

When devices receive this request, they discard it if their address does not match the destination IP address in the message. However, if it does match, they write their own hardware address into the destination MAC address field and send the message back to the source hardware address.

11.2.1 Setting ARP Timeout

Use the IP > ARP (Configure General) page to specify the timeout for ARP cache entries.

To configure the timeout for the ARP cache:

1. Click IP, ARP.
2. Select Configure General from the Step List.
3. Set the timeout to a suitable value for the ARP cache.
4. Click Apply.

Figure 11-2 Setting the ARP Timeout

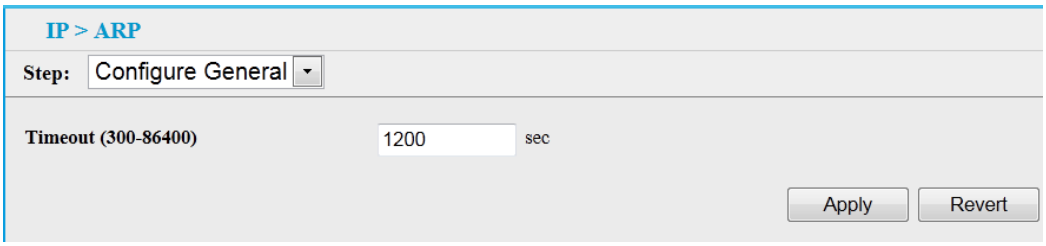


Table 11-2 Parameters of Setting the ARP Timeout

Title	Description
Timeout	Sets the aging time for dynamic entries in the ARP cache. (Range: 300 - 86400 seconds; Default: 1200 seconds) The ARP aging timeout can only be set globally for all VLANs.

----End

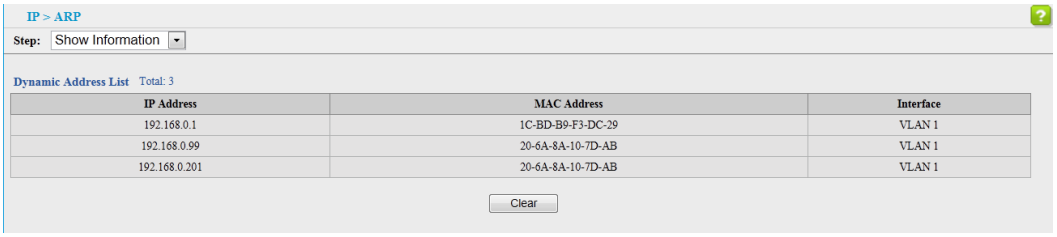
11.2.2 Displaying ARP Entries

Use the IP > ARP (Show Information) page to display dynamic or local entries in the ARP cache. The ARP cache contains entries for local interfaces, include host,mac address. However, most entries will be dynamically learned through replies to broadcast messages.

To display entries in the ARP cache:

1. Click IP, ARP.
2. Select Show Information from the Step List.

Figure 11-3 Displaying ARP Entries



----End

12 Multicast Configuration

About This Chapter

This chapter describes how to configure the following multicast services:

12.1 IGMP Snooping Configuration

12.1.1 Configuring IGMP Snooping and Query Parameters

Use the Multicast > IGMP Snooping > General page to configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards multicast traffic only to the ports that request it. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

To configure general settings for IGMP Snooping and Query:

1. Click Multicast, IGMP Snooping, General.
2. Adjust the IGMP settings as required.
3. Click Apply.

Figure 12-1 Configuring General Settings for IGMP Snooping

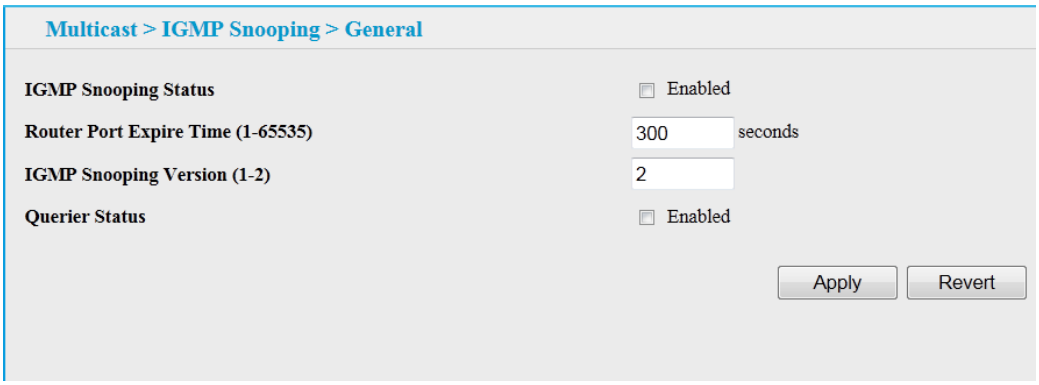


Table 12-1 Parameters of Configuring General Settings for IGMP Snooping

Title	Description
IGMP Snooping Status	When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Disabled) When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence. When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.
Router Port Expire Time	The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535, Recommended Range: 300-500 seconds, Default: 300)
IGMP Snooping Version	Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports. (Range: 1-2; Default: 2) This attribute configures the IGMP report/query version used by IGMP snooping. Versions 1 -2 are all supported, and versions 2 is backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.
Querier Status	When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled) Note: It is recommended that users turn on this feature, otherwise the receiving user report packets to configure a static multicast group does not generate table.

----End

12.1.2 Static Multicast Router

Use the Multicast > IGMP Snooping > Multicast Router (Add) page to statically attach an interface to a multicast router/switch.

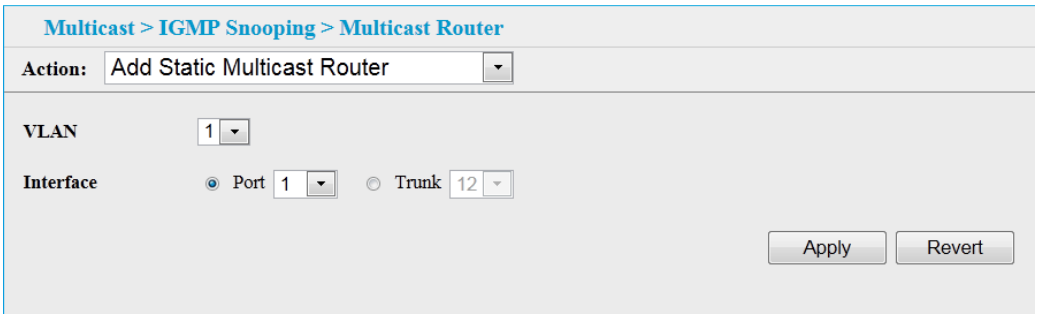
Depending on network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, the interface (and a specified VLAN) can be manually configured to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

To specify a static interface attached to a multicast router:

1. Click Multicast, IGMP Snooping, Multicast Router.
2. Select Add Static Multicast Router from the Action list.
3. Select the VLAN which will forward all the corresponding multicast traffic, and select the port or trunk attached to the multicast router.

4. Click Apply.

Figure 12-2 Configuring a Static Interface for a Multicast Router

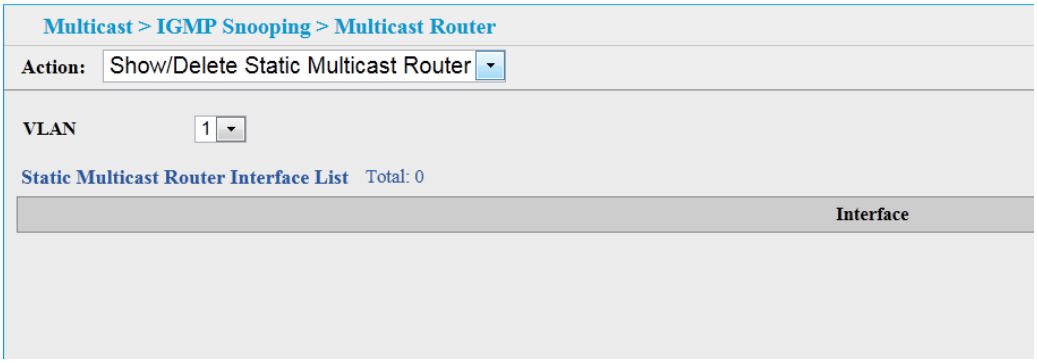


----End

To show/delete the static interfaces attached to a multicast router:

1. Click Multicast, IGMP Snooping, Multicast Router.
2. Select Show/delete Static Multicast Router from the Action list.
3. Select the VLAN for which to display this information.

Figure 12-3 Showing/Deleting Static Interfaces Attached a Multicast Router

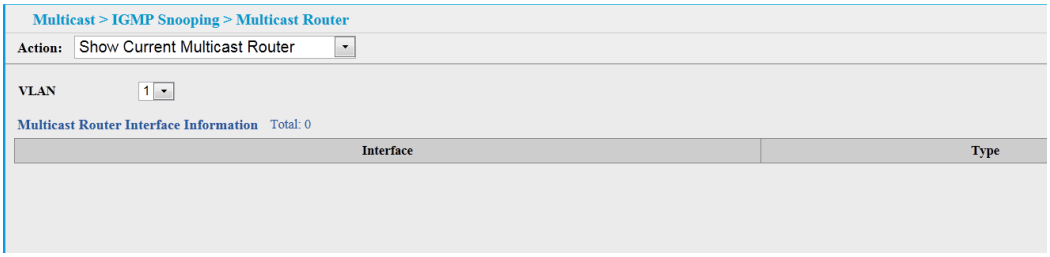


----End

To show the all interfaces attached to a multicast router:

1. Click Multicast, IGMP Snooping, Multicast Router.
2. Select Current Multicast Router from the Action list.
3. Select the VLAN for which to display this information.

Figure 12-4 Showing Current Static Interface Attached a Multicast Router



----End

Table 12-2 Parameters of Configuring Static Interface Attached Multicast Router

Title	Description
VLAN	Selects the VLAN which is to propagate all multicast traffic coming from the attached multicast router. (Range: 1-4093)
Interface	Activates the Port or Trunk scroll down list.
Type	Static or Dynamic

12.1.3 Assigning Interfaces to Multicast Services

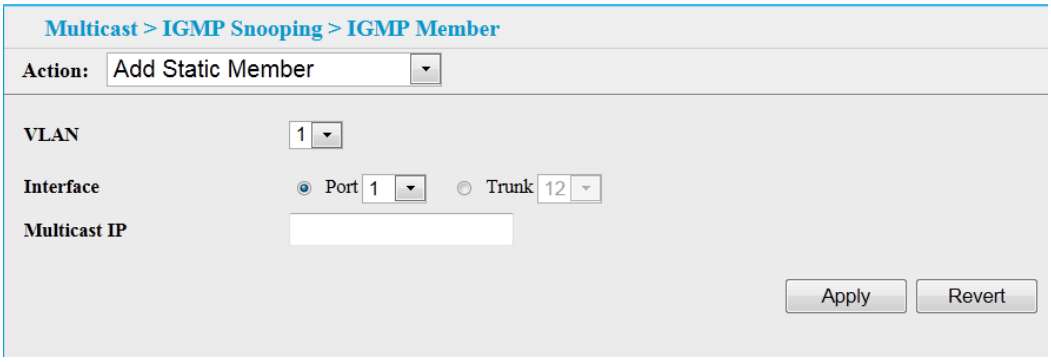
Use the Multicast > IGMP Snooping > IGMP Member (Add Static Member) page to statically assign a multicast service to an interface.

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages. However, for certain applications that require tighter control, it may be necessary to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

To statically assign an interface to a multicast service:

1. Click Multicast, IGMP Snooping, IGMP Member.
2. Select Add Static Member from the Action list.
3. Select the VLAN that will propagate the multicast service, specify the interface attached to a multicast service (through an IGMP-enabled switch or multicast router), and enter the multicast IP address.
4. Click Apply.

Figure 12-5 Assigning an Interface to a Multicast Service

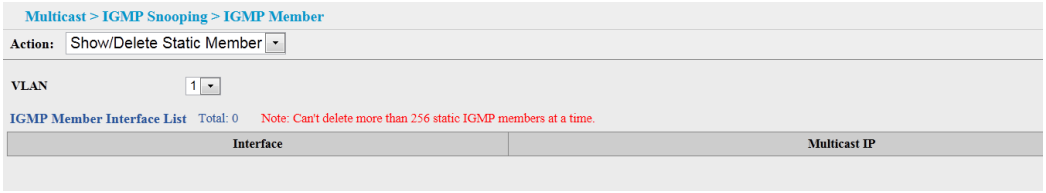


----End

To show/delete the static interfaces assigned to a multicast service:

1. Click Multicast, IGMP Snooping, IGMP Member.
2. Select Show/Delete Static Member from the Action list.
3. Select the VLAN for which to display this information.

Figure 12-6 Showing/Deleting Static Interfaces assigned to a Multicast Service

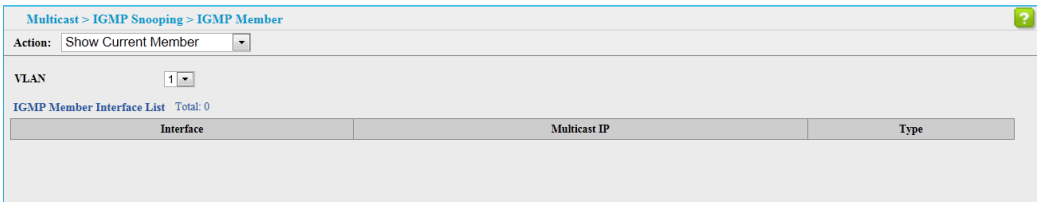


----End

To show the all interfaces statically or dynamically assigned to a multicast service:

1. Click Multicast, IGMP Snooping, IGMP Member.
2. Select Show Current Member from the Action list.
3. Select the VLAN for which to display this information.

Figure 12-7 Showing Current Interfaces assigned to a Multicast Service



----End

Table 12-3 Parameters of Configuring Interface assigned to a Multicast Service

Title	Description
VLAN	Specifies the VLAN which is to propagate the multicast service. (Range: 1-4093)
Interface	Activates the Port or Trunk scroll down list.
Port or Trunk	Specifies the interface assigned to a multicast group.
Multicast IP	The IP address for a specific multicast service.

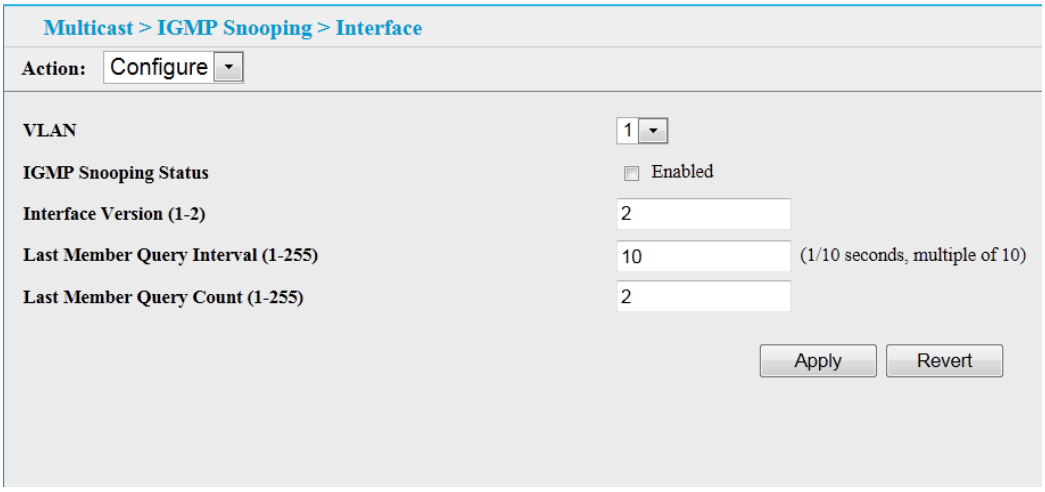
12.1.4 Setting IGMP Snooping Status per Interface

Use the Multicast > IGMP Snooping > Interface (Configure) page to configure IGMP snooping attributes for a VLAN interface.

To configure IGMP snooping on a VLAN:

1. Click Multicast, IGMP Snooping, Interface.
2. Select Configure from the Action list.
3. Select the VLAN to configure and update the required parameters.
4. Click Apply.

Figure 12-8 Configuring IGMP Snooping on an Interface



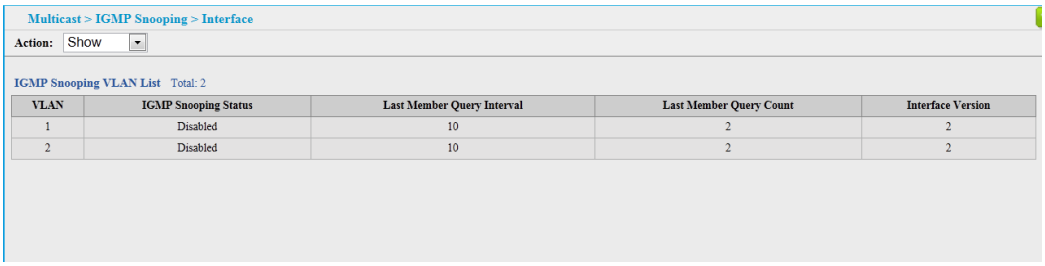
----End

To show the interface settings for IGMP snooping:

1. Click Multicast, IGMP Snooping, Interface.

2. Select Show from the Action list.

Figure 12-9 Showing Interface Settings for IGMP Snooping



----End

Table 12-4 Parameters of Configuring IGMP Snooping on an Interface

Title	Description
VLAN	ID of configured VLANs. (Range: 1-4093)
IGMP Snooping Status	When enabled, the switch will monitor network traffic on the indicated VLAN interface to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Disabled) When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence. When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.
Last Member Query Interval	The interval to wait for a response to a group-specific query message. (Range: 1-31744 tenths of a second in multiples of 10; Default: 1 second) When a multicast host leaves a group, it sends an IGMP leave message. When the leave message is received by the switch, it checks to see if this host is the last to leave the group by sending out an IGMP groupspecific query message, and starts a timer. If no reports are received before the timer expires, the group record is deleted, and a report is sent to the upstream multicast router. A reduced value will result in reduced time to detect the loss of the last member of a group or source, but may generate more burst traffic. This attribute will take effect only if IGMP snooping proxy reporting is enabled.
Last Member Query Count	The number of IGMP proxy groupspecific or query messages that are sent out before the system assumes there are no more local members. (Range: 1-255; Default: 2) This attribute will take effect only if IGMP snooping proxy reporting or IGMP querier is enabled.

Title	Description
Interface Version	Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports. (Range: 1-2; Default: 2) This attribute configures the IGMP report/query version used by IGMP snooping. Versions 1 - 2 are all supported, and versions 2 is backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.

12.1.5 Displaying Multicast Groups Discovered by IGMP Snoopoing

Use the Multicast > IGMP Snooping > Forwarding Entry page to display the forwarding entries learned through IGMP Snooping.

To show multicast groups learned through IGMP snooping:

1. Click Multicast, IGMP Snooping, Forwarding Entry.
2. Select the VLAN for which to display this information.

Figure 12-10 Showing Multicast Groups Learned by IGMP Snooping

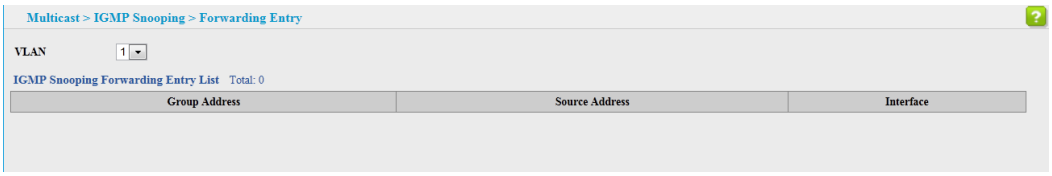


Table 12-5 Parameters of Showing Multicast Groups Learned by IGMP Snooping

Title	Description
VLAN	An interface on the switch that is forwarding traffic to downstream ports for the specified multicast group address.
Group Address	IP multicast group address with subscribers directly attached or downstream from the switch, or a static multicast group assigned to this interface.
Source Address	The address of one of the multicast servers transmitting traffic to the specified group.
Interface	A downstream port or trunk that is receiving traffic for the specified multicast group. This field may include both dynamically and statically configured multicast router ports.

----End