GS108T and GS110TP
Smart Switch
Software Administration Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

November 2010
202-10603-03
v2.0
©2010 NETGEAR, Inc. All rights reserved.
No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

Technical Support
Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at http://support.netgear.com.

Phone (US & Canada only): 1-888-NETGEAR
Phone (Other Countries): See Support information card.

Trademarks
NETGEAR, the NETGEAR logo, ReadyNAS, ProSafe, Smart Control Center, Auto Uplink, X-RAID2, and NeoTV are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT, and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions
To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

<table>
<thead>
<tr>
<th>Publication Part Number</th>
<th>Version</th>
<th>Publish Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>202-10603-03</td>
<td>v2.0</td>
<td>November 2010</td>
<td>• New SCC Features</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• IGMP Snooping Enhancements</td>
</tr>
<tr>
<td>202-10603-02</td>
<td>v1.0</td>
<td>April 2010</td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

Chapter 1  Getting Started

Getting Started with the GS108T and GS110TP Gigabit Smart Switches  . 9
Switch Management Interface ........................................... 10
Connecting the Switch to the Network ................................ 11
Switch Discovery in a Network with a DHCP Server ............... 12
Switch Discovery in a Network without a DHCP Server .......... 14
Configuring the Network Settings on the Administrative System 15
Web Access ........................................................................ 17
Smart Control Center Utilities ......................................... 18
   Network Utilities ......................................................... 18
   Configuration Upload and Download ................................ 19
   Firmware Upgrade ...................................................... 21
   Viewing and Managing Tasks ......................................... 22
Understanding the User Interfaces .................................... 24
   Using the Web Interface .............................................. 24
   Using SNMP ............................................................. 29
Interface Naming Convention ......................................... 30

Chapter 2  Configuring System Information

Management ..................................................................... 33
System Information ......................................................... 33
IP Configuration ............................................................. 34
Time .............................................................................. 36
Denial of Service ............................................................ 42
DNS ................................................................................. 44
Green Ethernet Configuration .......................................... 47
PoE (GS110TP Only) .......................................................... 48
   PoE Configuration ....................................................... 48
   PoE Port Configuration ................................................ 49
   Timer Global Configuration ......................................... 51
   Timer Schedule Configuration ..................................... 52
SNMP ............................................................................. 54
   SNMPV1/V2 ............................................................... 54
   Trap Flags .................................................................... 57
   SNMP v3 User Configuration ....................................... 58
LLDP ............................................................................... 59
   LLDP Configuration .................................................... 59
   LLDP Port Settings ....................................................... 61
   LLDP-MED Network Policy ......................................... 62
Chapter 3
Configuring Switching Information

LLDP-MED Port Settings .................................................. 64
Local Information ......................................................... 65
Neighbors Information ..................................................... 67
Services — DHCP Filtering .............................................. 72
DHCP Filtering Configuration .......................................... 72
Interface Configuration ................................................ 73

Ports ........................................................................... 76
Port Configuration ......................................................... 76
Flow Control ................................................................. 78
Link Aggregation Groups ................................................ 79
LAG Configuration ........................................................ 79
LAG Membership .......................................................... 81
LACP Configuration ....................................................... 82
LACP Port Configuration ................................................ 83
VLANs ......................................................................... 84
VLAN Configuration ....................................................... 84
VLAN Membership Configuration .................................. 86
Port VLAN ID Configuration .......................................... 87
Voice VLAN .................................................................. 89
Voice VLAN Properties .................................................. 89
Voice VLAN Port Setting ................................................. 90
Voice VLAN OUI ............................................................ 91
Auto-VoIP ..................................................................... 93
Spanning Tree Protocol ................................................... 94
STP Switch Configuration .............................................. 95
CST Configuration ........................................................ 97
CST Port Configuration .................................................. 98
CST Port Status ............................................................ 100
Rapid STP .................................................................... 101
MST Configuration ........................................................ 102
MST Port Configuration .................................................. 104
STP Statistics ................................................................. 106
Multicast ....................................................................... 108
Auto-Video Configuration ............................................. 108
IGMP Snooping .............................................................. 109
IGMP Snooping Querier .................................................. 117
Forwarding Database ..................................................... 121
MAC Address Table ....................................................... 121
Dynamic Address Configuration .................................. 123
Static MAC Address ...................................................... 124
Chapter 4
Configuring Quality of Service

Class of Service .......................................................... 126
  Basic CoS Configuration ........................................... 126
  CoS Interface Configuration ..................................... 128
  Interface Queue Configuration ................................... 129
  802.1p to Queue Mapping ........................................ 130
  DSCP to Queue Mapping ........................................... 131
Differentiated Services ................................................. 133
  Defining DiffServ .................................................. 133
  DiffServ Configuration ............................................ 134
  Class Configuration ............................................... 135
  Policy Configuration .............................................. 138
  Service Configuration ............................................ 138
  Service Statistics ................................................. 142

Chapter 5
Managing Device Security

Management Security Settings ....................................... 146
  Change Password .................................................. 146
  RADIUS Configuration ............................................ 147
  Configuring TACACS+ ............................................. 153
  Authentication List Configuration ............................. 155
Configuring Management Access ................................... 157
  HTTP Configuration ............................................... 157
  Secure HTTP Configuration ..................................... 158
  Certificate Download ............................................. 159
  Access Profile Configuration ................................... 161
  Access Rule Configuration ....................................... 162
Port Authentication ................................................... 164
  802.1X Configuration ............................................. 164
  Port Authentication ............................................... 165
  Port Summary ..................................................... 169
Traffic Control .......................................................... 171
  MAC Filter Configuration ....................................... 171
  MAC Filter Summary ............................................. 173
  Storm Control ..................................................... 174
  Port Security Configuration ..................................... 175
  Port Security Interface Configuration ....................... 176
  Security MAC Address .......................................... 178
  Protected Ports Membership .................................... 179
Configuring Access Control Lists .................................. 180
  ACL Wizard ......................................................... 180
  MAC ACL ............................................................ 182
  MAC Rules .......................................................... 183
Chapter 6
Monitoring the System

Ports ................................................................. 196
Switch Statistics ............................................... 196
Port Statistics .................................................. 198
Port Detailed Statistics ...................................... 199
EAP Statistics ................................................... 206
System Logs ..................................................... 208
Memory Logs .................................................. 208
FLASH Log Configuration .................................. 210
Server Log Configuration ................................... 212
Trap Logs ....................................................... 214
Event Logs ..................................................... 215
Port Mirroring ................................................ 216
Multiple Port Mirroring .................................... 216

Chapter 7
Maintaining the System

Reset ............................................................... 220
Device Reboot ................................................ 220
Factory Default ............................................. 221
Upload File From Switch ................................. 222
Download File To Switch .................................. 223
TFTP File Download .......................................... 223
HTTP File Download ....................................... 225
File Management ............................................. 228
Dual Image Configuration ................................. 228
Dual Image Status ........................................... 229
Troubleshooting .............................................. 231
Ping .............................................................. 231
Traceroute ....................................................... 232

Chapter 8
Accessing Help

Online Help ..................................................... 235
Support .......................................................... 235
User Guide ...................................................... 236
Appendix A  Hardware Specifications and Default Values

GS108T and GS110TP Gigabit Smart Switches Specifications ........ 238
GS108 Specifications ....................................................... 238
GS110 Specifications ....................................................... 238
GS108T and GS110TP Switch Performance ............................. 239
GS108T and GS110TP Switch Features and Defaults ................. 239
Port Characteristics ....................................................... 239
Traffic Control ......................................................... 240
Quality Of Service ...................................................... 240
Security ................................................................. 240
System Setup ......................................................... 241
Management ......................................................... 241
Other Features ......................................................... 242

Appendix B  Configuration Examples

Virtual Local Area Networks (VLANs) ................................. 244
VLAN Example Configuration ........................................... 245
Access Control Lists (ACLs) ............................................ 246
MAC ACL Example Configuration ...................................... 246
Standard IP ACL Example Configuration ............................ 248
Differentiated Services (DiffServ) ....................................... 249
Class ............................................................. 249
DiffServ Traffic Classes .................................................. 250
Creating Policies .......................................................... 250
DiffServ Example Configuration ....................................... 252
802.1X ............................................................. 254
802.1X Example Configuration ......................................... 255
MSTP ............................................................. 257
MSTP Example Configuration ........................................... 258

Appendix C  Notification of Compliance

Index
The NETGEAR® GS108T and GS110TP Smart Switch Software Administration Manual describes how to configure and operate the GS108T and GS110TP Gigabit Smart Switches by using the Web-based graphical user interface (GUI). This manual describes the software configuration procedures and explains the options available within those procedures.

Document Organization

The GS108T and GS110TP Smart Switch Software Administration Manual contains the following chapters:

- **Chapter 1, Getting Started**, contains information about performing the initial system configuration and accessing the user interface.
- **Chapter 2, Configuring System Information**, describes how to configure administrative features such as SNMP, DHCP, and port information.
- **Chapter 3, Configuring Switching Information**, describes how to manage and monitor the layer 2 switching features.
- **Chapter 4, Configuring Quality of Service**, describes how to manage the Access Control Lists (ACLs), and how to configure Differentiated Services and Class of Service features.
- **Chapter 5, Managing Device Security**, contains information about configuring switch security information such as port access control and RADIUS server settings.
- **Chapter 6, Monitoring the System**, describes how to view a variety of information about the switch and its ports, and to configure how the switch monitors events.
- **Chapter 7, Maintaining the System**, describes features to help you manage the switch.
- **Chapter 8, Accessing Help**, describes how to access Online Help resources for the switch.
- **Appendix A, Hardware Specifications and Default Values**, contains hardware specifications and default values on the GS108T and GS110TP Smart Switches.
- **Appendix B, Configuration Examples**, contains examples of how to configure various features on the GS108T and GS110TP Smart Switches, such as VLANs and ACLs.

**Note:** Refer to the release notes for the GS108T and GS110TP Gigabit Smart Switches for information about issues and workarounds.
Getting Started with the GS108T and GS110TP Gigabit Smart Switches

This chapter provides an overview of starting your NETGEAR GS108T or GS110TP Smart Switch and accessing the user interface. It also leads you through the steps to use the Smart Control Center utility. This chapter contains the following sections:

• Switch Management Interface on page 10
• Connecting the Switch to the Network on page 11
• Switch Discovery in a Network with a DHCP Server on page 12
• Switch Discovery in a Network without a DHCP Server on page 14
• Configuring the Network Settings on the Administrative System on page 15
• Web Access on page 17
• Smart Control Center Utilities on page 18
• Understanding the User Interfaces on page 24
• Interface Naming Convention on page 30
Switch Management Interface

The NETGEAR GS108T and GS110TP Smart Switches contain an embedded Web server and management software for managing and monitoring switch functions. The GS108T and GS110TP function as simple switches without the management software. However, you can use the management software to configure more advanced features that can improve switch efficiency and overall network performance.

Web-based management lets you monitor, configure, and control your switch remotely using a standard Web browser instead of using expensive and complicated SNMP software products. From your Web browser, you can monitor the performance of your switch and optimize its configuration for your network. You can configure all switch features, such as VLANs, QoS, and ACLs by using the Web-based management interface.

NETGEAR provides the Smart Control Center utility with this product. This program runs under Microsoft® Windows® XP, Windows 2000, or Windows Vista® and provides a front end that discovers the switches on your network segment (L2 broadcast domain). When you power up your switch for the first time, use the Smart Control Center to discover the switch and view the network information that has been automatically assigned to the switch by a DHCP server; or, if no DHCP server is present on the network, use the Smart Control Center to discover the switch and assign static network information.

In addition to enabling NETGEAR switch discovery, the Smart Control Center provides several utilities to help you maintain the NETGEAR switches on your network, such as password management, firmware upgrade, and configuration file backup. For more information, see Smart Control Center Utilities on page 18.
Connecting the Switch to the Network

To enable remote management of the switch through a Web browser or SNMP, you must connect the switch to the network and configure it with network information (an IP address, subnet mask, and default gateway). The switch has a default IP address of 192.168.0.239 and a default subnet mask of 255.255.255.0.

Use one of the following three methods to change the default network information on the switch:

- **Dynamic assignment through DHCP**—DHCP is enabled by default on the switch. If you connect the switch to a network with a DHCP server, the switch obtains its network information automatically. You can use the Smart Control Center to discover the automatically-assigned network information. For more information, see *Switch Discovery in a Network with a DHCP Server* on page 12.

- **Static assignment through the Smart Control Center**—If you connect the switch to a network that does not have a DHCP server, you can use the Smart Control Center to assign a static IP address, subnet mask, and default gateway. For more information, see *Switch Discovery in a Network without a DHCP Server* on page 14.

- **Static assignment by connecting from a local host**—If you do not want to use the Smart Control Center to assign a static address, you can connect to the switch from a host (administrative system) in the 192.168.0.0/24 network and change the settings by using the Web-based management interface on the switch. For information about how to set the IP address on the administrative system so it is in the same subnet as the default IP address of the switch, see *Configuring the Network Settings on the Administrative System* on page 15.
Switch Discovery in a Network with a DHCP Server

This section describes how to set up your switch in a network that has a DHCP server. The DHCP client on the switch is enabled by default. When you connect it to your network, the DHCP server will automatically assign an IP address to your switch. Use the Smart Control Center to discover the IP address automatically assigned to the switch.

To install the switch in a network with a DHCP server, use the following steps:

1. Connect the switch to a network with a DHCP server.
2. Power on the switch by connecting its AC-DC power adapter. For the GS108T, you can also power on the switch by connecting Port 1 to a PoE Power Sourcing Equipment (PSE).
3. Install the Smart Control Center on your computer.
4. Start the Smart Control Center.
5. Click Discover for the Smart Control Center to find your switch. You should see a screen similar to the one shown in Figure 1.

![Figure 1. Smart Switch Discovery](image-url)
6. Make a note of the displayed IP address assigned by the DHCP server. You will need this value to access the switch directly from a Web browser (without using the Smart Control Center).

<table>
<thead>
<tr>
<th>Product</th>
<th>MAC Address</th>
<th>IP Address</th>
<th>System</th>
<th>Location</th>
<th>DHCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>GS108Tv2</td>
<td>00:12:6b:21:5c:96-49</td>
<td>10.131.12.174</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7. Select your switch by clicking the line that displays the switch, then click the Web Browser Access button. The Smart Control Center displays a login window similar to the following figure.

Use your Web browser to manage your switch. The default password is password. Then use this page to proceed to management of the switch covered in Using the Web Interface on page 24.
Switch Discovery in a Network without a DHCP Server

This section describes how to use the Smart Control Center to set up your switch in a network without a DHCP server. If your network has no DHCP service, you must assign a static IP address to your switch. If you choose, you can assign it a static IP address, even if your network has DHCP service.

To assign a static IP address:

1. Connect the switch to your existing network.
2. Power on the switch by plugging in the AC-DC power adapter. For the GS108T, you can also power on the switch by connecting Port 1 to a PoE PSE.
3. Install the Smart Control Center on your computer.
4. Start the Smart Control Center.
5. Click Discover for the Smart Control Center to find your GS108T or GS110TP switch. The utility broadcasts Layer 2 discovery packets within the broadcast domain to discover the switch. You should see a screen similar to Figure 1 on page 12.
6. Select the switch, then click Configure Device. The page expands to display additional fields at the bottom of the page, as the following figure shows.

7. Choose the Disabled radio box to disable DHCP.
8. Enter the static switch IP address, gateway IP address and subnet mask, and then type your password and click Apply.
Tip: You must enter the current password every time you use the Smart Control Center to update the switch setting. The default password is password.

Please ensure that your PC and the switch are in the same subnet. Make a note of these settings for later use.

Configuring the Network Settings on the Administrative System

If you choose not to use the Smart Control Center to configure the network information on the switch, you can connect directly to the switch from an administrative system, such as a PC or laptop computer. The IP address of the administrative system must be in the same subnet as the default IP address on the switch. For most networks, this means you must change the IP address of the administrative system to be on the same subnet as the default IP address of the switch (192.168.0.239).

To change the IP address on an administrative system running a Microsoft® Windows® operating system, open the Internet Protocol (TCP/IP) properties screen that you access from the Local Area Connection properties, as shown in the following figure. You need Windows Administrator privileges to change these settings.
WARNING!

When you change the IP address of your administrative system, you will lose your connection to the rest of the network. Be sure to write down your current network address settings before you change them.

To modify the network settings on your administrative system:

1. On your PC, access the MS Windows operating system TCP/IP Properties.
2. Set the IP address of the administrative system to an address in the 192.168.0.0 network, such as 192.168.0.200. The IP address must be different from that of the switch but within the same subnet.
3. Click OK.

To configure a static address on the switch:

1. Use a straight-through cable to connect the Ethernet port on the administrative system directly to any port on the GS108T or GS110TP.
2. Open a Web browser on your PC and connect to the management interface as described in Web Access on page 17.
3. Change the network settings on the switch to match those of your network (this procedure is described in IP Configuration on page 34).

After you change the network settings on the switch, return the network configuration on your administrative system to the original settings.
Web Access

To access the GS108T or GS110TP management interface, use one of the following methods:

- From the Smart Control Center, select the switch and click **Web Browser Access**.
- Open a Web browser and enter the IP address of the switch in the address field.

You must be able to ping the IP address of the GS108T or GS110TP management interface from your administrative system for Web access to be available. If you used the Smart Control Center to set up the IP address and subnet mask, either with or without a DHCP server, use that IP address in the address field of your Web browser. If you did not change the IP address of the switch from the default value, enter 192.168.0.239 into the address field.

Clicking **Web Browser Access** on the Smart Control Center or accessing the switch directly from your Web browser displays the login screen shown in the following figure.

Figure 2. Login Screen
Smart Control Center Utilities

In addition to device discovery and network address assignment, the Smart Control Center includes several maintenance features. This section describes the following Smart Control Center utilities:

- **Network Utilities** on page 18
- **Configuration Upload and Download** on page 19
- **Firmware Upgrade** on page 21
- **Viewing and Managing Tasks** on page 22

Network Utilities

From the **Network** tab, you can perform the following functions:

- **DHCP Refresh**—Forces the switch to release the current bindings and request new address information from the DHCP server.
- **Reboot Device**—Reboots the selected device.
- **Web Browser Access**—Launches a Web browser and connects to the management interface for the selected device.
- **Configure Device**—Allows you to modify network information for the switch, including the IP address, DHCP client mode, system name, and location. For more information about this feature, see Configuring the Device.
- **Change Password**—Allows you to set a new password for the device. For more information about this feature, see Changing the Switch Password.

Configuring the Device

To modify switch information:

1. Select the switch.
2. Click **Configure Device**. Additional fields appear on the screen.

   ![Configuration Interface](image)

   Define the basic configuration.

3. To assign or update a static IP address, default gateway, or subnet mask, disable the DHCP client and enter the new information. You can also specify a system name and location for the switch.
4. Type the password in the **Current Password** field. You cannot apply the changes without a valid switch password. The default password for the switch is *password*.
5. Click **Apply** to update the switch with the changes to the network information.
Changing the Switch Password

1. Select the switch.

![Changing the Switch Password Form]

3. Type the switch password in the Current Password field. The default password for the switch is password.
4. Type the new password in the New Password and Confirm Password fields. The password can contain up to 20 ASCII characters.
5. Click Apply to update the switch with the new password.

Configuration Upload and Download

When you make changes to the switch, the configuration information is stored in a file on the switch. You can backup the configuration by uploading the configuration file from the switch to an administrative system. You can download a saved configuration file from the administrative system to the switch. The configuration file you download to the switch overwrites the running configuration on the switch.

Configuration upload and download is useful if you want to save a copy of the current switch configuration (Upload Configuration) before you make changes. If you do not like the changes, you can use the Download Configuration option to restore the switch to the settings in the saved configuration file.

To save a copy of the current switch configuration on your administrative system:

1. Click the Maintenance tab and select the device with the configuration to save.
2. Click Upload Configuration.
3. From the Browse for Folder window that appears, navigate to and select the folder where you want to store the configuration file.
4. Click OK.
5. Enter the switch password and click **Apply**.

The file is uploaded to the administrative computer as a *.cfg file. You can open it and view the contents with a text editor.

To restore the configuration to a previously saved version:

1. Click the **Maintenance** tab and select the device with the configuration to restore.
2. Click **Download Configuration**.
3. From the **Select a Configuration** window that appears, navigate to and select the configuration file to download to the switch.
4. Click **Open**.
5. Enter the switch password and click **Apply** to begin the download process.

Optionally, you can schedule a different date and time to download the configuration file. To delay the download process, clear the **Run Now?** check box and enter a date and time to complete the download.

---

**Note:** Click the **Tasks** tab to view status information about the configuration download.
Firmware Upgrade

The application software for the GS108T and GS110TP Smart Switches is upgradeable, enabling your switch to take advantage of improvements and additional features as they become available. The upgrade procedure and the required equipment are described in this section. This procedure assumes that you have downloaded or otherwise obtained the firmware upgrade and that you have it available as a binary file on your computer. This procedure uses the TFTP protocol to implement the transfer from computer to switch.

---

**Note:** You can also upgrade the firmware using the TFTP Download and HTTP Download features mentioned in this book. See Download File To Switch on page 223.

---

To upgrade your firmware:

1. Click the **Maintenance** tab, and then click the **Firmware** link directly below the tabs (see Figure 1 on page 12).
2. Select the switch to upgrade and click **Download Firmware**.
3. From the **Select new firmware** window that appears, navigate to and select the firmware image to download to the switch.
4. Click **Open**.

---

![Download Firmware dialog box](image)
By default, the firmware is downloaded to primary storage and will be become the active image after the download completes and the switch reboots. To download firmware to use as a backup image, select the Secondary Storage option. To prevent the switch from using the downloaded firmware as the active image, make sure the Run this FW after download option is clear.

Note: NETGEAR recommends that you download the same image as the primary and secondary image for redundancy.

5. Click Apply.

6. Enter the switch password to continue downloading the firmware.
   Optionally, you can schedule a different date and time to download and install the firmware image. To delay the upgrade process, clear the Run Now? check box and enter a date and time to complete the upgrade.

7. Click Apply to download the firmware and upgrade the switch with the new image.

8. When the process is complete, the switch automatically reboots.

Note: Click the Tasks tab to view status information about the firmware upgrade.

WARNING!

It is important that you do not power-off the administrative system or the switch while the firmware upgrade is in progress.

Viewing and Managing Tasks

From the Tasks tab, you can view information about configuration downloads and firmware upgrades that have already occurred, are in progress, or are scheduled to take place at a later time. You can also delete or reschedule selected tasks. The following figure shows the Tasks page.
The following list describes the command buttons that are specific to the **Tasks** page:

- **Delete Task**—Remove a completed or schedule task from the list.
- **Reschedule**—Change the scheduled date and time for a pending firmware upgrade or configuration download.
- **Select Range**—Select all tasks that occurred or are scheduled to occur within a certain period of time.
Understanding the User Interfaces

The switch software includes a set of comprehensive management functions for configuring and monitoring the system by using one of the following methods:

- Web user interface
- Simple Network Management Protocol (SNMP)

Each of the standards-based management methods allows you to configure and monitor the components of the switch software. The method you use to manage the system depends on your network size and requirements, and on your preference.

The GS108T and GS110TP Smart Switch Software Administration Manual describes how to use the Web-based interface to manage and monitor the system.

Using the Web Interface

To access the switch by using a Web browser, the browser must meet the following software requirements:

- HTML version 4.0, or later
- HTTP version 1.1, or later
- Java Runtime Environment 1.6 or later

Use the following procedures to log on to the Web interface:

1. Open a Web browser and enter the IP address of the switch in the Web browser address field.
2. The factory default password is **password**. Type the password into the field on the login screen, as shown in Figure 2 on page 17, and then click **Login**. Passwords are case sensitive.
3. After the system authenticates you, the System Information page displays. Figure 3 on page 25 shows the layout of the Smart Switch Web interface.
The navigation tabs along the top of the Web interface give you quick access to the various switch functions. The tabs are always available and remain constant, regardless of which feature you configure.

When you select a tab, the features for that tab appear as links directly under the tabs. The feature links in the blue bar change according to the navigation tab that is selected.

The configuration pages for each feature are available as links in the page menu on the left side of the page. Some items in the menu expand to reveal multiple configuration pages, as Figure 4 on page 26 shows. When you click a menu item that includes multiple configuration pages, the item becomes preceded by a down arrow symbol and expands to display the additional pages.

**Figure 3. Administrative Page Layout**

*Navigation Tabs, Feature Links, and Page Menu*

The navigation tabs along the top of the Web interface give you quick access to the various switch functions. The tabs are always available and remain constant, regardless of which feature you configure.

When you select a tab, the features for that tab appear as links directly under the tabs. The feature links in the blue bar change according to the navigation tab that is selected.

The configuration pages for each feature are available as links in the page menu on the left side of the page. Some items in the menu expand to reveal multiple configuration pages, as Figure 4 on page 26 shows. When you click a menu item that includes multiple configuration pages, the item becomes preceded by a down arrow symbol and expands to display the additional pages.
Configuration and Monitoring Options

The area directly under the feature links and to the right of the page menu displays the configuration information or status for the page you select. On pages that contain configuration options, you can input information into fields or select options from drop-down menus.

Each page contains access to the HTML-based help that explains the fields and configuration options for the page. Each page also contains command buttons.

The following table shows the command buttons that are used throughout the pages in the Web interface:

<table>
<thead>
<tr>
<th>Button</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Clicking <strong>Add</strong> adds the new item configured in the heading row of a table.</td>
</tr>
<tr>
<td>Apply</td>
<td>Clicking the <strong>Apply</strong> button sends the updated configuration to the switch. Configuration changes take effect immediately.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Clicking <strong>Cancel</strong> cancels the configuration on the screen and resets the data on the screen to the latest value of the switch.</td>
</tr>
<tr>
<td>Delete</td>
<td>Clicking <strong>Delete</strong> removes the selected item.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Clicking the <strong>Refresh</strong> button refreshes the page with the latest information from the device.</td>
</tr>
<tr>
<td>Logout</td>
<td>Clicking the <strong>Logout</strong> button ends the session.</td>
</tr>
</tbody>
</table>

Device View

The Device View is a Java® applet that displays the ports on the switch. This graphic provides an alternate way to navigate to configuration and monitoring options. The graphic also provides information about device ports, current configuration and status, table information, and feature components.

The Device View is available from the **System > Device View** page.

The port coloring indicates whether a port is currently active. Green indicates that the port is enabled, red indicates that an error has occurred on the port, or red indicates that the link is disabled.
The following figure shows the Device View of the GS108T.

![Device View of GS108T](image1)

The following figure shows the Device View of the GS110TP.

![Device View of GS110TP](image2)

Click the port you want to view or configure to see a menu that displays statistics and configuration options. Click the menu option to access the page that contains the configuration or monitoring options.
If you click the graphic, but do not click a specific port, the main menu appears, as the following figure shows. This menu contains the same option as the navigation tabs at the top of the page.

![Menu graphic]

**Help Page Access**

Every page contains a link to the online help, which contains information to assist in configuring and managing the switch. The online help pages are context sensitive. For example, if the IP Addressing page is open, the help topic for that page displays if you click Help. Figure 3 on page 25 shows the location of the link to the Help Page on the Web interface.

**User-Defined Fields**

User-defined fields can contain 1 to 159 characters, unless otherwise noted on the configuration Web page. All characters may be used except for the following (unless specifically noted in for that feature):

* Table 1: *

```
/    <
/    >|  
*    |  
?    
```
Using SNMP

The switch software supports the configuration of SNMP groups and users that can manage traps that the SNMP agent generates.

Switch switches use both standard public MIBs for standard functionality and private MIBs that support additional switch functionality. All private MIBs begin with a “-” prefix. The main object for interface configuration is in -SWITCHING-MIB, which is a private MIB. Some interface configurations also involve objects in the public MIB, IF-MIB.

SNMP is enabled by default. The System > Management > System Information Web page, which is the page that displays after a successful login, displays the information you need to configure an SNMP manager to access the switch.

Any user can connect to the switch using the SNMPv3 protocol, but for authentication and encryption, the switch supports only one user which is admin; therefore there is only one profile that can be created or modified.

To configure authentication and encryption settings for the SNMPv3 admin profile by using the Web interface:

1. Navigate to the System > SNMP > SNMPv3 > User Configuration page.
2. To enable authentication, select an Authentication Protocol option, which is either MD5 or SHA.
3. To enable encryption, select the DES option in the Encryption Protocol field. Then, enter an encryption code of eight or more alphanumeric characters in the Encryption Key field.
4. Click Apply.

To access configuration information for SNMPv1 or SNMPv2, click System > SNMP > SNMPv1/v2 and click the page that contains the information to configure.
# Interface Naming Convention

The switch supports physical and logical interfaces. Interfaces are identified by their type and the interface number. The physical ports are gigabit interfaces and are numbered on the front panel. You configure the logical interfaces by using the software. The following table describes the naming convention for all interfaces available on the switch.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>The physical ports are gigabit Ethernet interfaces and are numbered sequentially starting from one.</td>
<td>g1, g2, g3</td>
</tr>
<tr>
<td>Link Aggregation Group (LAG)</td>
<td>LAG interfaces are logical interfaces that are only used for bridging functions.</td>
<td>i1, i2, i3 LAG1, LAG2</td>
</tr>
<tr>
<td>CPU Management Interface</td>
<td>This is the internal switch interface responsible for the switch base MAC address. This interface is not configurable and is always listed in the MAC Address Table.</td>
<td>c1</td>
</tr>
</tbody>
</table>
Use the features in the System tab to define the switch’s relationship to its environment. The System tab contains links to the following features:

- Management on page 33
- PoE (GS110TP Only) on page 48
- SNMP on page 54
- LLDP on page 59
- Services — DHCP Filtering on page 72
Management

This section describes how to display the switch status and specify some basic switch information, such as the management interface IP address, system clock settings, and DNS information. From the Management link, you can access the following pages:

- System Information on page 33
- IP Configuration on page 34
- Time on page 36
- Denial of Service on page 42
- DNS on page 44
- Green Ethernet Configuration on page 47

System Information

After a successful login, the System Information page displays. Use this page to configure and view general device information.

To display the System Information page, click System > Management > System Information. A screen similar to the following displays.

To define system information:
1. Open the System Information page.
2. Define the following fields:
   - System Name. Enter the name you want to use to identify this switch. You may use up to 31 alphanumeric characters. The factory default is blank.
• **System Location.** Enter the location of this switch. You may use up to 31 alphanumeric characters. The factory default is blank.

• **System Contact.** Enter the contact person for this switch. You may use up to 31 alphanumeric characters. The factory default is blank.

3. Click **Apply**.

   The system parameters are applied, and the device is updated.

The following table describes the status information the System Page displays.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>The serial number of the switch.</td>
</tr>
<tr>
<td>System Object ID</td>
<td>The base object ID for the switch’s enterprise MIB.</td>
</tr>
<tr>
<td>Date &amp; Time</td>
<td>The current date and time.</td>
</tr>
<tr>
<td>System Up Time</td>
<td>Displays the number of days, hours, and minutes since the last system restart.</td>
</tr>
<tr>
<td>Base MAC Address</td>
<td>The universally assigned network address.</td>
</tr>
<tr>
<td>Model Name</td>
<td>The model name of the switch.</td>
</tr>
<tr>
<td>Boot Version</td>
<td>The boot code version of the switch.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The software version of the switch.</td>
</tr>
</tbody>
</table>

**IP Configuration**

Use the IP Configuration page to configure network information for the management interface, which is the logical interface used for in-band connectivity with the switch through any of the switch’s front panel ports. The configuration parameters associated with the switch’s network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

To access the page, click **System > Management > IP Configuration**. A screen similar to the following displays.
To configure the network information for the management interface:

1. Select the appropriate radio button to determine how to configure the network information for the switch management interface:
   - **Dynamic IP Address (DHCP)**. Specifies that the switch must obtain the IP address through a DHCP server.
   - **Dynamic IP Address (BOOTP)**. Specifies that the switch must obtain the IP address through a BootP server.
   - **Static IP Address**. Specifies that the IP address, subnet mask, and default gateway must be manually configured. Enter this information in the fields below this radio button.

2. If you selected the Static IP Address option, configure the following network information:
   - **IP Address**. The IP address of the network interface. The factory default value is 192.168.0.239. Each part of the IP address must start with a number other than zero. For example, IP addresses 001.100.192.6 and 192.001.10.3 are not valid.
   - **Subnet Mask**. The IP subnet mask for the interface. The factory default value is 255.255.255.0.
   - **Default Gateway**. The default gateway for the IP interface. The factory default value is 192.168.0.254.

3. Specify the VLAN ID for the management VLAN.

   The management VLAN is used to establish an IP connection to the switch from a workstation that is connected to a port in the same VLAN. If not specified, the active management VLAN ID is 1 (default), which allows an IP connection to be established through any port.

   When the management VLAN is set to a different value, an IP connection can be made only through a port that is part of the management VLAN. It is also mandatory that the
port VLAN ID (PVID) of the port to be connected in that management VLAN be the same as the management VLAN ID.

The management VLAN has the following requirements:

- Only one management VLAN can be active at a time.
- When a new management VLAN is configured, connectivity through the existing management VLAN is lost.
- The management station should be reconnected to the port in the new management VLAN.

**Note:** Make sure that the VLAN to be configured as the management VLAN exists. And make sure that the PVID of at least one port that is a port of the VLAN is the same as the management VLAN ID. For information about creating VLANs and configuring the PVID for a port, see *VLANs* on page 84.

4. If you change any of the network connection parameters, click **Apply** to apply the changes to the system.

5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

**Time**

Switch software supports the Simple Network Time Protocol (SNTP). You can also set the system time manually

SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. Switch software operates only as an SNTP client and cannot provide time services to other systems.

Time sources are established by Stratums. Stratums define the accuracy of the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock. The device receives time from stratum 1 and above since it is itself a stratum 2 device.

The following is an example of stratums:

- **Stratum 0:** A real-time clock is used as the time source, for example, a GPS system.
- **Stratum 1:** A server that is directly linked to a Stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.
- **Stratum 2:** The time source is distanced from the Stratum 1 server over a network path. For example, a Stratum 2 server receives the time over a network link, via NTP, from a Stratum 1 server.

Information received from SNTP servers is evaluated based on the time level and server type.
SNTP time definitions are assessed and determined by the following time levels:

- **T1**: Time at which the original request was sent by the client.
- **T2**: Time at which the original request was received by the server.
- **T3**: Time at which the server sent a reply.
- **T4**: Time at which the client received the server's reply.

The device can poll Unicast server types for the server time.

Polling for Unicast information is used for polling a server for which the IP address is known. SNTP servers that have been configured on the device are the only ones that are polled for synchronization information. T1 through T4 are used to determine server time. This is the preferred method for synchronizing device time because it is the most secure method. If this method is selected, SNTP information is accepted only from SNTP servers defined on the device using the SNTP Server Configuration page.

The device retrieves synchronization information, either by actively requesting information or at every poll interval.

**Time Configuration**

Use the Time Configuration page to view and adjust date and time settings.

To display the Time Configuration page, click **System > Management > Time > SNTP Global Configuration**.
To configure the time by using the CPU clock cycle as the source:

1. From the Clock Source field, select **Local**.
2. In the **Date** field, enter the date in the DD/MM/YYYY format.
3. In the **Time** field, enter the time in HH:MM:SS format.

**Note:** If you do not enter a date and time, the switch will calculate the date and time using the CPU’s clock cycle.

When the Clock Source is set to **Local**, the **Time Zone** field is grayed out (disabled):

4. Click **Apply** to send the updated configuration to the switch. Configuration changes occur immediately.

To configure the time through SNTP:

1. From the Clock Source field, select **SNTP**.

   When the **Clock Source** is set to SNTP, the Date and Time fields are grayed out (disabled). The switch gets the date and time from the network.

2. Use the menu to select the Coordinated Universal Time (UTC) time zone in which the switch is located, expressed as the number of hours. The options in the Time Zone menu specify the time difference from UTC time zone.

3. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

4. Use the **SNTP Server Configuration** page to configure the SNTP server settings, as described in **SNTP Server Configuration** on page 39.

5. Click **Refresh** to refresh the page with the most current data from the switch.

6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

The SNTP Global Status table on the **Time Configuration** page displays information about the system’s SNTP client. The following table describes the SNTP Global Status fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Specifies the SNTP Version the client supports.</td>
</tr>
<tr>
<td>Supported Mode</td>
<td>Specifies the SNTP modes the client supports. Multiple modes may be supported by a client.</td>
</tr>
<tr>
<td>Last Update Time</td>
<td>Specifies the local date and time (UTC) the SNTP client last updated the system clock.</td>
</tr>
<tr>
<td>Last Attempt Time</td>
<td>Specifies the local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.</td>
</tr>
</tbody>
</table>
Click **Refresh** to refresh the page with the most current data from the switch.

**SNTP Server Configuration**

Use the SNTP Server Configuration page to view and modify information for adding and modifying Simple Network Time Protocol SNTP servers.

To display the SNTP Server Configuration page, click **System > Management > Time > SNTP Server Configuration**.
To configure a new SNTP Server:

1. Enter the appropriate SNTP server information in the available fields:
   - **Server Type**. Specifies whether the address for the SNTP server is an IP address (IPv4) or hostname (DNS).
   - **Address**. Enter the IP address or the hostname of the SNTP server.
   - **Port**. Enter a port number on the SNTP server to which SNTP requests are sent. The valid range is 1–65535. The default is 123.
   - **Priority**. Specifies the priority of this server entry in determining the sequence of servers to which SNTP requests are sent. Enter a priority from 1–3, with 1 being the default and the highest priority. Servers with lowest numbers have priority.
   - **Version**. Enter the protocol version number. The range is 1–4.

2. Click **Add**.

3. Repeat the previous steps to add additional SNTP servers. You can configure up to three SNTP servers.

4. To removing an SNTP server, select the check box next to the configured server to remove, and then click **Delete**. The entry is removed, and the device is updated.

5. To change the settings for an existing SNTP server, select the check box next to the configured server and enter new values in the available fields, and then click **Apply**. Configuration changes take effect immediately.

6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
The SNTP Server Status table displays status information about the SNTP servers configured on your switch. The following table describes the SNTP Global Status fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Specifies all the existing Server Addresses. If no Server configuration exists, a message saying “No SNTP server exists” flashes on the screen.</td>
</tr>
<tr>
<td>Last Update Time</td>
<td>Specifies the local date and time (UTC) that the response from this server was used to update the system clock.</td>
</tr>
<tr>
<td>Last Attempt Time</td>
<td>Specifies the local date and time (UTC) that this SNTP server was last queried.</td>
</tr>
<tr>
<td>Last Attempt Status</td>
<td>Specifies the status of the last SNTP request to this server. If no packet has been received from this server, a status of Other is displayed:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Other</strong>: None of the following enumeration values.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Success</strong>: The SNTP operation was successful and the system time was updated.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Request Timed Out</strong>: A directed SNTP request timed out without receiving a response from the SNTP server.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bad Date Encoded</strong>: The time provided by the SNTP server is not valid.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Version Not Supported</strong>: The SNTP version supported by the server is not compatible with the version supported by the client.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Server Unsynchronized</strong>: The SNTP server is not synchronized with its peers. This is indicated via the ‘leap indicator’ field on the SNTP message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Server Kiss Of Death</strong>: The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.</td>
</tr>
<tr>
<td>Requests</td>
<td>Specifies the number of SNTP requests made to this server since last agent reboot.</td>
</tr>
<tr>
<td>Failed Requests</td>
<td>Specifies the number of failed SNTP requests made to this server since last reboot.</td>
</tr>
</tbody>
</table>

Click **Refresh** to refresh the page with the most current data from the switch.
Denial of Service

Use the Denial of Service (DoS) page to configure DoS control. The switch software provides support for classifying and blocking specific types of DoS attacks. You can configure your system to monitor and block six types of attacks:

- **SIP=DIP**: Source IP address = Destination IP address.
- **First Fragment**: TCP Header size is smaller than the configured value.
- **TCP Fragment**: IP Fragment Offset = 1.
- **TCP Flag**: TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port**: Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP**: Limiting the size of ICMP Ping packets.

Auto-DoS Configuration

The **Auto-DoS Configuration** page lets you automatically enable all the DoS features available on the switch, except for the L4 Port attack. See the previous section for information about the types of DoS attacks the switch can monitor and block.

To access the **Auto-DoS Configuration** page, click System > Management > Denial of Service > Auto-DoS Configuration.

To configure the Auto-DoS feature:

1. Select a radio button to enable or disable Auto-DoS:
   - **Disable**: Auto-DoS is disabled (default).
   - **Enable**: Auto-DoS is enabled.

2. Click **Apply** to send the updated configuration to the switch. Configuration changes occur immediately.

3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
**DoS Configuration**

The DoS Configuration page lets you to select which types of DoS attacks for the switch to monitor and block.

To access the DoS Configuration page, click System > Management > Denial of Service > DoS Configuration.

To configure individual DoS settings:

1. Select the types of DoS attacks for the switch to monitor and block and configure any associated values, as the following list describes.
   - **Denial of Service SIP=DIP.** Enable or disable this option by selecting the appropriate radio button. Enabling SIP=DIP DoS prevention causes the switch to drop packets that have a source IP address equal to the destination IP address. The factory default is Disable.
   - **Denial of Service First Fragment.** Enable or disable this option by selecting the appropriate radio button. Enabling First Fragment DoS prevention causes the switch to drop packets that have a TCP header smaller than the configured Min TCP Hdr Size. The factory default is Disable.
   - **Denial of Service Min TCP Hdr Size.** Specify the Min TCP Hdr Size allowed. If First Fragment DoS prevention is enabled, the switch will drop packets that have a TCP header smaller than this configured Min TCP Hdr Size. The factory default is 20 bytes.
   - **Denial of Service TCP Fragment.** Enable or disable this option by selecting the appropriate radio button. Enabling TCP Fragment DoS prevention causes the switch to drop packets that have an IP fragment offset equal to 1. The factory default is Disable.
   - **Denial of Service TCP Flag.** Enable or disable this option by selecting the appropriate radio button. Enabling TCP Flag DoS prevention causes the switch to...
drop packets that have TCP flag SYN set and TCP source port less than 1024 or TCP control flags set to 0 and TCP sequence number set to 0 or TCP flags FIN, URG, and PSH set and TCP sequence number set to 0 or both TCP flags SYN and FIN set. The factory default is Disable.

- **Denial of Service L4 Port.** Enable or disable this option by selecting the appropriate radio button. Enabling L4 Port DoS prevention causes the switch to drop packets that have TCP/UDP source port equal to TCP/UDP destination port. The factory default is Disable.

- **Denial of Service ICMP.** Enable or disable this option by selecting the appropriate radio button. Enabling ICMP DoS prevention causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMP packet size. The factory default is Disable.

- **Denial of Service Max ICMP Size.** Specify the Max ICMP packet size allowed. If ICMP DoS prevention is enabled, the switch will drop ICMP ping packets that have a size greater than this configured Max ICMP packet size. The factory default is Disable.

2. If you change any of the DoS settings, click **Apply** to apply the changes to the switch.

3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

**DNS**

You can use these pages to configure information about DNS servers the network uses and how the switch operates as a DNS client.

**DNS Configuration**

Use this page to configure global DNS settings and DNS server information.

To access this page, click **System > Management > DNS > DNS Configuration**.
To configure the global DNS settings

1. Specify whether to enable or disable the administrative status of the DNS Client.
   - **Enable.** Allow the switch to send DNS queries to a DNS server to resolve a DNS domain name.
   - **Disable.** Prevent the switch from sending DNS queries.

2. Enter the DNS default domain name to include in DNS queries. When the system is performing a lookup on an unqualified hostname, this field is provided as the domain name (for example, if default domain name is netgear.com and the user enters test, then test is changed to test.netgear.com to resolve the name).

3. To specify the DNS server to which the switch sends DNS queries, enter an IP address in standard IPv4 dot notation in the **DNS Server Address** and click **Add**. The server appears in the list below. You can specify up to eight DNS servers. The precedence is set in the order created.

4. To remove a DNS server from the list, select the check box next to the server you want to remove and click **Delete**. If no DNS server is specified, the check box is global and will delete all the DNS servers listed.

5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

6. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

**Host Configuration**

Use this page to manually map host names to IP addresses or to view dynamic DNS mappings.

To access this page, click **System > Management > DNS > Host Configuration**.
To add a static entry to the local DNS table:

1. Specify the static host name to add. Enter up to 158 characters.
2. Specify the IP address in standard IPv4 dot notation to associate with the hostname.
3. Click Add. The entry appears in the list below.
4. To remove an entry from the static DNS table, select the check box next to the entry and click Delete.
5. To change the hostname or IP address in an entry, select the check box next to the entry and enter the new information in the appropriate field, and then click Apply.
6. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

The Dynamic Host Configuration table shows host name-to-IP address entries that the switch has learned. The following table describes the dynamic host fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Lists the host name you assign to the specified IP address.</td>
</tr>
<tr>
<td>Total</td>
<td>Amount of time since the dynamic entry was first added to the table.</td>
</tr>
<tr>
<td>Elapsed</td>
<td>Amount of time since the dynamic entry was last updated.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of the dynamic entry.</td>
</tr>
<tr>
<td>Addresses</td>
<td>Lists the IP address associated with the host name.</td>
</tr>
</tbody>
</table>

Click Refresh to refresh the table with the most current data from the switch.

Click Clear to delete Dynamic Host Entries. The table will be repopulated with entries as they are learned.
Green Ethernet Configuration

Use this page to configure Green Ethernet features. Using the Green Ethernet features allows for power consumption savings.

To access this page, click System > Management > Green Ethernet Configuration.

To configure the Green Ethernet feature:

1. Enable or disable the **Short Cable Mode**.
   - **Enable**. The switch performs a cable test on each cable connect to its ports. If the cable is less than 10m in length, the port is placed in low power mode (nominal power).
   - **Disable**. Full transmit power is provided to all ports, regardless of cable length.

2. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
PoE (GS110TP Only)

Ports g1–g8 on the GS110TP are IEEE802.3af-compliant ports. Each port is capable of delivering up to 15.4W of reliable, uninterrupted power to connected PoE-powered devices (PD). The GS110TP can provide a total of 46W of power to all connected devices. You can configure per-port priority settings, timers, and power limits to manage the power supplied to the connected PDs and to ensure that the GS110TP power budget is used effectively.

From the PoE link under the System tab, you can view and configure PoE settings for the switch and for ports g1–g8.

From the PoE link, you can access the following pages:

- PoE Configuration on page 48
- PoE Port Configuration on page 49
- Timer Global Configuration on page 51
- Timer Schedule Configuration on page 52

PoE Configuration

Use the PoE Configuration page to view global PoE power information and to configure PoE SNMP trap settings.

To display the PoE Configuration page, click System > PoE > Basic > PoE Configuration.

**Note:** You can also access the PoE Configuration page by clicking System > PoE > Advanced > PoE Configuration.
To configure PoE trap settings:

1. Select the appropriate radio button to enable or disable SNMP traps.
2. Click **Apply** to apply the new settings to the system.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. Click **Refresh** to update the screen with the current information.

The PoE Configuration page also provides the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Status</td>
<td>Indicates whether the PoE capability is on or off.</td>
</tr>
<tr>
<td>Nominal Power</td>
<td>Indicates the nominal amount of power the switch can provide to all ports.</td>
</tr>
<tr>
<td>Threshold Power</td>
<td>Shows the amount of power the system can consume before the system will not provide power to an additional port.</td>
</tr>
<tr>
<td>Consumed Power</td>
<td>Shows the total amount of power currently being delivered to all ports.</td>
</tr>
</tbody>
</table>

**PoE Port Configuration**

Use the PoE Port Configuration page to configure per-port PoE settings.

To display the PoE Port Configuration page, click **System > PoE > Advanced > PoE Port Configuration**.

To configure PoE Port settings:

1. To configure settings for a physical port, click **PORTS**.
2. To configure settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure settings for both physical ports and LAGs, click **ALL**.

4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.

5. Configure or view the settings:
   - **Admin Mode.** Enable or disable the ability of the port to deliver power.
   - **Priority Level.** Determine which ports can deliver power if the total power delivered by the switch crosses a certain threshold. The switch may not be able to supply power to all connected devices. Priority is used to determine which ports can supply power. When ports have the same priority, the lower numbered port is given a higher priority.
   - **Detection Mode.** Select the detection mode to be used on the port. The detection mode can be one of the following modes:
     - **Legacy Only:** Select this option if only Legacy (capacitive signature) PDs need to be detected.
     - **802.3af 2point Only:** Select this option if only IEEE 802.3af (resistive signature) PDs need to be detected using two collected samples. This is the default mode.
     - **802.3af 4point Only:** Select this option if only IEEE 802.3af (resistive signature) PDs need to be detected using four collected samples.
     - **802.3af 2point and Legacy:** Select this option to use both Legacy and IEEE 802.3af 2point methods to detect PDs.
     - **802.3af 4point and Legacy:** Select this option to use both Legacy and IEEE 802.3af 2point methods to detect PDs.
   - **Class.** View the class of the PD connected to the port. The class defines the range of power a PD is drawing from the system. The class is defined as:
     - **0:** 0.44–12.95W
     - **1:** 0.44–3.83W
     - **2:** 3.84–6.48W
     - **3:** 6.49–12.95W
     - **4:** Reserved
   - **Timer Schedule.** Select the timer schedule to use for the port. By default, no timer schedules are configured. To create a timer schedule, use the Timer Global Configuration page.
   - **Output Voltage.** Shows the current voltage being delivered to device in Volts.
   - **Output Current.** Shows the current being delivered to device in mA.
   - **Output Power.** Shows the current power being delivered to device in Watts.
   - **Power Limit Type.** Select the type of power limit to use on the port, which is one of the following:
     - **Class:** Select this option to base the power limit on the detected class value. When this value is selected, the user-configured value configured in the Power Limit field is ignored.
• **User**: Select this option to base the power limit on the value configured in the Power Limit field.

• **Power Limit**: Set the maximum amount of power that can be delivered by a port.

• **Status**: View the operational status of the port PD detection.
  - **Disabled**: Indicates no power is being delivered.
  - **DeliveringPower**: Indicates power is being drawn by a connected device.
  - **Fault**: Indicates a problem with the port.
  - **Test**: Indicates the port is in test mode.
  - **OtherFault**: Indicates the port is idle due to an error condition.
  - **Searching**: Indicates the port is not in one of the above states.

6. Click **Apply** to apply the new settings to the system.

7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

8. Click **Refresh** to update the screen with the current information.

## Timer Global Configuration

Use the Timer Global Configuration page to create or remove timers and to control the administrative status of the feature. Timers control when power can and cannot be delivered to the port. Use the following general steps to add a timer to a port:

1. Create the timer on the Timer Global Configuration page.
2. Configure the timer settings on the Timer Schedule Configuration page.
3. Assign the timer to the port or LAG on the PoE Port Configuration page.

---

**Note**: The Timer Schedule feature must be enabled for the settings to be applied to the ports.

---

To display the Timer Global Configuration page, click **System > PoE > Advanced > Timer Global Configuration**.
To configure global timer settings:

1. To add a timer, enter a name in the Timer Schedule Name field, and click **Add**.
2. To remove a timer, select the check box associated with the timer and click **Delete**.
3. To enable or disable the timer feature, select the appropriate radio button and click **Apply**.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

**Timer Schedule Configuration**

Use the Timer Schedule Configuration page to configure when the power to a port is turned off. For example, you can specify that the power is turned off every night, during the weekend, or during the same one-week period every year.

To display the Timer Schedule Configuration page, click **System > PoE > Advanced > Timer Schedule Configuration**.
To configure timer schedules:

1. Select the name of the schedule created on the Timer Global Configuration page.
2. Specify the time to turn off power. The time range is from 00:00 to 23:59.
3. Specify the day to turn off power by clicking the calendar icon and selecting the date.
4. If required, specify the end date by clicking the calendar icon and selecting the date.
5. If required, use the Recurrence Pattern and Daily Mode fields to customize the power shutdown schedule.
6. Click Apply to save the settings for the selected timer.
7. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
SNMP

From SNMP link under the System tab, you can configure SNMP settings for SNMP V1/V2 and SNMPv3.

From the SNMP link, you can access the following pages:

- **SNMPV1/V2** on page 54
- **Trap Flags** on page 57
- **SNMP v3 User Configuration** on page 58

**SNMPV1/V2**

The pages under the SNMPV1/V2 menu allow you to configure SNMP community information, traps, and trap flags.

**Community Configuration**

To display this page, click **System > SNMP > SNMP V1/V2 > Community Configuration**.

By default, two SNMP Communities exist:

- Private, with Read/Write privileges and status set to **Enable**.
- Public, with Read Only privileges and status set to **Enable**.

These are well-known communities. Use this page to change the defaults or to add other communities. Only the communities that you define using this page will have access to the switch using the SNMPv1 and SNMPv2c protocols. Only those communities with read/write level access can be used to change the configuration using SNMP.

Use this page when you are using the SNMPv1 and SNMPv2c protocol.
To configure SNMP communities:

1. To add a new SNMP community, enter community information in the available fields described below, and then click **Add**.
   - **Management Station IP**. Specify the IP address of the management station. Together, the Management Station IP and the Management Station IP Mask denote a range of IP addresses from which SNMP clients may use that community to access this device. If either (Management Station IP or Management Station IP Mask) value is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's address is ANDed with the mask, as is the Management Station IP Address; and, if the values are equal, access is allowed. For example, if the Management Station IP and Management Station IP Mask parameters are 192.168.1.0/255.255.255.0, then any client whose address is 192.168.1.0 through 192.168.1.255 (inclusive) will be allowed access. To allow access from only one station, use a Management Station IP Mask value of 255.255.255.255, and use that machine's IP address for Client Address.
   - **Management Station IP Mask**. Specify the subnet mask to associate with the management station IP address.
   - **Community String**. Specify a community name. A valid entry is a case-sensitive string of up to 16 characters.
   - **Access Mode**. Specify the access level for this community by selecting Read/Write or Read Only from the menu.
   - **Status**. Specify the status of this community by selecting Enable or Disable from the pull down menu. If you select Enable, the Community Name must be unique among all valid Community Names or the set request will be rejected. If you select Disable, the Community Name will become invalid.

2. To modify an existing community, select the check box next to the community, change the desired fields, and then click **Apply**. Configuration changes take effect immediately.

3. To delete a community, select the check box next to the community and click **Delete**.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

**Trap Configuration**

This page displays an entry for every active Trap Receiver. To access this page, click **System > SNMP > SNMP V1/V2 > Trap Configuration**.
To configure SNMP trap settings:

1. To add a host that will receive SNMP traps, enter trap configuration information in the available fields described below, and then click **Add**.
   - **Recipients IP.** The address in x.x.x.x format to receive SNMP traps from this device.
   - **Version.** The trap version to be used by the receiver from the menu.
     - SNMP v1: Uses SNMP v1 to send traps to the receiver.
     - SNMP v2: Uses SNMP v2 to send traps to the receiver.
   - **Community String.** The community string for the SNMP trap packet to be sent to the trap manager. This may be up to 16 characters and is case sensitive.
   - **Status.** Select the receiver’s status from the menu:
     - Enable: Send traps to the receiver.
     - Disable: Do not send traps to the receiver.

2. To modify information about an existing SNMP recipient, select the check box next to the recipient, change the desired fields, and then click **Apply.** Configuration changes take effect immediately.

3. To delete a recipient, select the check box next to the recipient and click **Delete.**

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
Trap Flags

The pages in the Trap Manager folder allow you to view and configure information about SNMP traps the system generates.

Use the Trap Flags page to enable or disable traps the switch can send to an SNMP manager. When the condition identified by an active trap is encountered by the switch, a trap message is sent to any enabled SNMP Trap Receivers, and a message is written to the trap log.

To access the Trap Flags page, click System > SNMP > SNMP V1/V2 > Trap Flags.

To configure the trap flags:

1. From the Authentication field, enable or disable activation of authentication failure traps by selecting the corresponding button. The factory default is Enable.
2. From the Link Up/Down field, enable or disable activation of link status traps by selecting the corresponding button. The factory default is Enable.
3. From the Spanning Tree field, enable or disable activation of spanning tree traps by selecting the corresponding button. The factory default is Enable.
4. If you make any changes to this page, click Apply to send the updated configuration to the switch. Configuration changes take effect immediately.
5. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
SNMP v3 User Configuration

This is the configuration for SNMP v3.

To access this page, click System > SNMP > SNMP V3 > User Configuration.

The SNMPv3 Access Mode is a read-only field that shows the access privileges for the user account. The admin account always has Read/Write access, and all other accounts have Read Only access.

To configure SNMPv3 settings for the user account:

1. In the Authentication Protocol field, specify the SNMPv3 Authentication Protocol setting for the selected user account. The valid Authentication Protocols are None, MD5, or SHA. If you select:
   - **None**: The user will be unable to access the SNMP data from an SNMP browser.
   - **MD5 or SHA**: The user login password will be used as SNMPv3 authentication password, and you must therefore specify a password. The password must be eight characters in length.

2. In the Encryption Protocol field, choose whether to encrypt SNMPv3 packets transmitted by the switch.
   - **None**: Do not encrypt the contents of SNMPv3 packets transmitted from the switch.
   - **DES**: Encrypt SNMPv3 packets using the DES encryption protocol.

3. If you selected DES in the Encryption Protocol field, enter the SNMPv3 Encryption Key here. Otherwise, this field is ignored. Valid keys are 0 to 15 characters long.

4. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
LLDP

The IEEE 802.1AB-defined standard, Link Layer Discovery Protocol (LLDP), allows stations on an 802 LAN to advertise major capabilities and physical descriptions. This information is viewed by a network manager to identify system topology and detect bad configurations on the LAN.

From the LLDP link, you can access the following pages:

- **LLDP Configuration** on page 59
- **LLDP Port Settings** on page 61
- **LLDP-MED Network Policy** on page 62
- **LLDP-MED Port Settings** on page 64
- **Local Information** on page 65
- **Neighbors Information** on page 67

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function. The transmit and receive functions can be enabled/disabled separately per port. By default, both transmit and receive are disabled on all ports. The application is responsible for starting each transmit and receive state machine appropriately, based on the configured status and operational state of the port.

The Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) is an enhancement to LLDP with the following features:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority, and DiffServ settings), enabling plug and play networking.
- Device location discovery for creation of location databases.
- Extended and automated power management of Power over Ethernet endpoints.
- Inventory management, enabling network administrators to track their network devices and determine their characteristics (manufacturer, software and hardware versions, serial/asset number).

LLDP Configuration

Use the LLDP Configuration page to specify LLDP and LLDP-MED parameters that are applied to the switch.

To display the LLDP Configuration page, click **System > LLDP > Basic > LLDP Configuration**.
To configure global LLDP settings:

1. Configure the following LLDP properties.
   - **TLV Advertised Interval.** Specify the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 1–32768 seconds.
   - **Hold Multiplier.** Specify multiplier on the transmit interval to assign to Time-to-Live (TTL). The default is 4, and the range is 2–10.
   - **Reinitializing Delay.** Specify the delay before a reinitialization. The default is 2 seconds, and the range is 1–10 seconds.
   - **Transmit Delay.** Specify the interval for the transmission of notifications. The default is 5 seconds, and the range is 5–3600 seconds.

2. To change the LLDP-MED properties in the **Fast Start Duration** field, specify the number of LLDP packets sent when the LLDP-MED Fast Start mechanism is initialized, which occurs when a new endpoint device links with the LLDP-MED network connectivity device. The default value is 3, and the range is from 1–10.

3. Click **Apply** to apply the new settings to the system.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

5. Click **Refresh** to update the screen with the current information.
LLDP Port Settings

Use the LLDP Port Settings page to specify LLDP parameters that are applied to a specific interface.

To display the LLDP Port Settings page, click System > LLDP > Advanced > LLDP Port Settings.

To configure LLDP port settings:

1. Change the LLDP port settings described below:
   - **Interface.** Specifies the port to be affected by these parameters.
   - **Admin Status.** Select the status for transmitting and receiving LLDP packets:
     - **Tx Only:** Enable only transmitting LLDP PDUs on the selected ports.
     - **Rx Only:** Enable only receiving LLDP PDUs on the selected ports.
     - **Tx and Rx:** Enable both transmitting and receiving LLDP PDUs on the selected ports.
     - **Disabled:** Do not transmit or receive LLDP PDUs on the selected ports.
   - **Management IP Address.** Choose whether to advertise the management IP address from the interface. The possible field values are:
     - **Stop Advertise:** Do not advertise the management IP address from the interface.
     - **Auto Advertise:** Advertise the current IP address of the device as the management IP address.
   - **Notification.** When notifications are enabled, LLDP interacts with the Trap Manager to notify subscribers of remote data change statistics. The default is Disabled.
• **Optional TLV(s).** Enable or disable the transmission of optional type-length value (TLV) information from the interface. The TLV information includes the system name, system description, system capabilities, and port description. To configure the System Name, see *Management* on page 33. To configure the Port Description, see *Ports* on page 76.

2. If you make any changes to the page, click **Apply** to apply the new settings to the system.

3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

### LLDP-MED Network Policy

This page displays information about the LLPD-MED network policy TLV transmitted in the LLDP frames on the selected local interface.

To display this page, click **System > LLDP > Advanced > LLDP-MED Network Policy**.
From the **Interface** menu, select the interface with the information to view. The following table describes the LLDP-MED network policy information that displays on the screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Policy Number</td>
<td>Specifies the policy number.</td>
</tr>
<tr>
<td>Application</td>
<td>Specifies the media application type associated with the policy, which can</td>
</tr>
<tr>
<td></td>
<td>be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td></td>
<td>• Voice</td>
</tr>
<tr>
<td></td>
<td>• Guest Voice</td>
</tr>
<tr>
<td></td>
<td>• Guest Voice Signaling</td>
</tr>
<tr>
<td></td>
<td>• Softphone Voice</td>
</tr>
<tr>
<td></td>
<td>• Video Conferencing</td>
</tr>
<tr>
<td></td>
<td>• Streaming Video</td>
</tr>
<tr>
<td></td>
<td>• Video Signaling</td>
</tr>
<tr>
<td></td>
<td>A port can receive multiple application types. The application information</td>
</tr>
<tr>
<td></td>
<td>is displayed only if a network policy TLV has been transmitted from the</td>
</tr>
<tr>
<td></td>
<td>port.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Specifies the VLAN ID associated with the policy.</td>
</tr>
<tr>
<td>VLAN Type</td>
<td>Specifies whether the VLAN associated with the policy is tagged or</td>
</tr>
<tr>
<td></td>
<td>untagged.</td>
</tr>
<tr>
<td>User Priority</td>
<td>Specifies the priority associated with the policy.</td>
</tr>
<tr>
<td>DSCP</td>
<td>Specifies the DSCP associated with a particular policy type.</td>
</tr>
</tbody>
</table>

Click **Refresh** to refresh the page with the most current data from the switch.
LLDP-MED Port Settings

Use this page to enable LLDP-MED mode on an interface and configure its properties.

To display this page, click System > LLDP > Advanced > LLDP-MED Port Settings.

To configure LLDP-MED settings for a port:

1. From the Port field, select the port to configure.
2. From the LLDP-MED Status field, enable or disable the LLDP-MED mode for the selected interface.
3. From the Notification field, specify whether the port should send a topology change notification if a device is connected or removed.
4. From the Transmit Optional TLVs field, specify whether the port should transmit optional type length values (TLVs) in the LLDP PDU frames. If enabled, the following LLDP-MED TLVs are transmitted:
   - MED Capabilities
   - Network Policy
   - Location Identification
   - Extended Power via MDI: PSE
   - Extended Power via MDI: PD
   - Inventory
5. Click Apply to send the updated configuration to the switch. These changes occur immediately and the configuration will be saved.
6. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
Local Information

Use the LLDP Local Information page to view the data that each port advertises through LLDP.

To display the LLDP Local Device Information page, click **System > Advanced > LLDP > Local Information**.

The following table describes the LLDP local information that displays for each port.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Select the interface with the information to display.</td>
</tr>
<tr>
<td>Port ID Subtype</td>
<td>Identifies the type of data displayed in the Port ID field.</td>
</tr>
<tr>
<td>Port ID</td>
<td>Identifies the physical address of the port.</td>
</tr>
<tr>
<td>Port Description</td>
<td>Identifies the user-defined description of the port. To configure the Port Description, see <em>Ports</em> on page 76.</td>
</tr>
<tr>
<td>Advertisement</td>
<td>Displays the advertisement status of the port.</td>
</tr>
</tbody>
</table>

Click **Refresh** to refresh the page with the most current data from the switch.

To view additional details about a port, click the name of the port in the Interface column of the Port Information table.
A popup window displays information for the selected port.

![Port Information](image)

The following table describes the detailed local information that displays for the selected port.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Address</td>
<td>Displays the type of address the management interface uses, such as an IPv4 address.</td>
</tr>
<tr>
<td>Address SubType</td>
<td>Displays the type of address the management interface uses, such as an IPv4 address.</td>
</tr>
<tr>
<td>Address</td>
<td>Displays the address used to manage the device.</td>
</tr>
<tr>
<td>Interface SubType</td>
<td>Displays the port subtype.</td>
</tr>
<tr>
<td>Interface Number</td>
<td>Displays the number that identifies the port.</td>
</tr>
<tr>
<td>Auto-Negotiation Supported</td>
<td>Specifies whether the interface supports port-speed auto-negotiation. The possible values are True or False.</td>
</tr>
<tr>
<td>Auto-Negotiation Enabled</td>
<td>Displays the port speed auto-negotiation support status. The possible values are True (enabled) or False (disabled).</td>
</tr>
<tr>
<td>Auto Negotiation Advertised Capabilities</td>
<td>Displays the port speed auto-negotiation capabilities such as 1000BASE-T half-duplex mode or 100BASE-TX full-duplex mode.</td>
</tr>
<tr>
<td>Operational MAU Type</td>
<td>Displays the Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interface collision detection and bit injection into the network.</td>
</tr>
</tbody>
</table>
Use the LLDP Neighbors Information page to view the data that a specified interface has received from other LLDP-enabled systems.

To display the LLDP Neighbors Information page, click System > LLDP > Advanced > Neighbors Information.
The following table describes the information that displays for all LLDP neighbors that have been discovered.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSAP Entry</td>
<td>Displays the Media Service Access Point (MSAP) entry number for the remote device.</td>
</tr>
<tr>
<td>Local Port</td>
<td>Displays the interface on the local system that received LLDP information from a remote system.</td>
</tr>
<tr>
<td>Chassis ID Subtype</td>
<td>Identifies the type of data displayed in the Chassis ID field on the remote system.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>Identifies the remote 802 LAN device's chassis.</td>
</tr>
<tr>
<td>Port ID Subtype</td>
<td>Identifies the type of data displayed in the remote system's Port ID field.</td>
</tr>
<tr>
<td>Port ID</td>
<td>Identifies the physical address of the port on the remote system from which the data was sent.</td>
</tr>
<tr>
<td>System Name</td>
<td>Identifies the system name associated with the remote device. If the field is blank, the name might not be configured on the remote system.</td>
</tr>
</tbody>
</table>

Click **Refresh** to update the information on the screen with the most current data.

To view additional information about the remote device, click the link in the MSAP Entry field.

A popup window displays information for the selected port.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port Details</strong></td>
<td></td>
</tr>
<tr>
<td>Local Port</td>
<td>Displays the interface on the local system that received LLDP information from a remote system.</td>
</tr>
<tr>
<td>MSAP Entry</td>
<td>Displays the Media Service Access Point (MSAP) entry number for the remote device.</td>
</tr>
<tr>
<td><strong>Basic Details</strong></td>
<td></td>
</tr>
<tr>
<td>Chassis ID Subtype</td>
<td>Identifies the type of data displayed in the <strong>Chassis ID</strong> field on the remote system.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>Identifies the remote 802 LAN device's chassis.</td>
</tr>
<tr>
<td>Port ID Subtype</td>
<td>Identifies the type of data displayed in the remote system's <strong>Port ID</strong> field.</td>
</tr>
<tr>
<td>Port ID</td>
<td>Identifies the physical address of the port on the remote system from which the data was sent.</td>
</tr>
<tr>
<td>Port Description</td>
<td>Identifies the user-defined description of the port.</td>
</tr>
<tr>
<td>System Name</td>
<td>Identifies the system name associated with the remote device.</td>
</tr>
<tr>
<td>System Description</td>
<td>Specifies the description of the selected port associated with the remote system.</td>
</tr>
<tr>
<td>System Capabilities</td>
<td>Specifies the system capabilities of the remote system.</td>
</tr>
<tr>
<td><strong>Managed Addresses</strong></td>
<td></td>
</tr>
<tr>
<td>Address SubType</td>
<td>Specifies the type of the management address.</td>
</tr>
<tr>
<td>Address</td>
<td>Specifies the advertised management address of the remote system.</td>
</tr>
<tr>
<td>Interface SubType</td>
<td>Specifies the port subtype.</td>
</tr>
<tr>
<td>Interface Number</td>
<td>Identifies the port on the remote device that sent the information.</td>
</tr>
<tr>
<td><strong>MAC/PHY Details</strong></td>
<td></td>
</tr>
<tr>
<td>Auto-Negotiation Supported</td>
<td>Specifies whether the remote device supports port-speed auto-negotiation. The possible values are True or False</td>
</tr>
<tr>
<td>Auto-Negotiation Enabled</td>
<td>Displays the port speed auto-negotiation support status. The possible values are True or False</td>
</tr>
<tr>
<td>Auto Negotiation Advertised Capabilities</td>
<td>Displays the port speed auto-negotiation capabilities.</td>
</tr>
<tr>
<td>Operational MAU Type</td>
<td>Displays the Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interface collision detection and bit injection into the network.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>MED Details</strong></td>
<td></td>
</tr>
<tr>
<td>Capabilities Supported</td>
<td>Specifies the supported capabilities that were received in MED TLV from the device.</td>
</tr>
<tr>
<td>Current Capabilities</td>
<td>Specifies the advertised capabilities that were received in MED TLV from the device.</td>
</tr>
<tr>
<td>Device Class</td>
<td>Displays the LLDP-MED endpoint device class. The possible device classes are:</td>
</tr>
<tr>
<td></td>
<td>• Endpoint Class 1 Indicates a generic endpoint class, offering basic LLDP services.</td>
</tr>
<tr>
<td></td>
<td>• Endpoint Class 2 Indicates a media endpoint class, offering media streaming capabilities as well as all Class 1 features.</td>
</tr>
<tr>
<td></td>
<td>• Endpoint Class 3 Indicates a communications device class, offering all Class 1 and Class 2 features plus location, 911, Layer 2 switch support and device information management capabilities.</td>
</tr>
<tr>
<td>PoE Device Type</td>
<td>Displays the port PoE type. For example, Powered.</td>
</tr>
<tr>
<td>PoE Power Source</td>
<td>Displays the port's power source.</td>
</tr>
<tr>
<td>PoE Power Priority</td>
<td>Displays the port's power priority.</td>
</tr>
<tr>
<td>PoE Power Value</td>
<td>Displays the port's power value.</td>
</tr>
<tr>
<td>Hardware Revision</td>
<td>Displays the hardware version advertised by the remote device.</td>
</tr>
<tr>
<td>Firmware Revision</td>
<td>Displays the firmware version advertised by the remote device.</td>
</tr>
<tr>
<td>Software Revision</td>
<td>Displays the software version advertised by the remote device.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Displays the serial number advertised by the remote device.</td>
</tr>
<tr>
<td>Model Name</td>
<td>Displays the model name advertised by the remote device.</td>
</tr>
<tr>
<td>Asset ID</td>
<td>Displays the asset ID advertised by the remote device.</td>
</tr>
<tr>
<td><strong>Location Information</strong></td>
<td></td>
</tr>
<tr>
<td>Civic</td>
<td>Displays the physical location, such as the street address, the remote device has advertised in the location TLV. For example, 123 45th St. E. The field value length range is 6–160 characters.</td>
</tr>
<tr>
<td>Coordinates</td>
<td>Displays the location map coordinates the remote device has advertised in the location TLV, including latitude, longitude and altitude.</td>
</tr>
<tr>
<td>ECS ELIN</td>
<td>Displays the Emergency Call Service (ECS) Emergency Location Identification Number (ELIN) the remote device has advertised in the location TLV. The field range is 10–25.</td>
</tr>
<tr>
<td>Unknown</td>
<td>Displays unknown location information for the remote device.</td>
</tr>
</tbody>
</table>
### Network Policies

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Type</td>
<td>Specifies the media application type associated with the policy advertised by the remote device.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Specifies the VLAN ID associated with the policy.</td>
</tr>
<tr>
<td>VLAN Type</td>
<td>Specifies whether the VLAN associated with the policy is tagged or untagged.</td>
</tr>
<tr>
<td>User Priority</td>
<td>Specifies the priority associated with the policy.</td>
</tr>
<tr>
<td>DSCP</td>
<td>Specifies the DSCP associated with a particular policy type.</td>
</tr>
</tbody>
</table>

### LLDP Unknown TLVs

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Displays the unknown TLV type field.</td>
</tr>
<tr>
<td>Value</td>
<td>Displays the unknown TLV value field.</td>
</tr>
</tbody>
</table>
Services — DHCP Filtering

DHCP Filtering is a useful feature that can be employed as a security measure against unauthorized DHCP servers. A known attack is when an unauthorized DHCP server responds to a client that is requesting an IP address. The server configures the gateway for the client to be equal to the IP address of the server. At that point, the client sends all of its IP traffic destined to other networks to the unauthorized machine. This gives the attacker the possibility of snooping traffic for passwords or employing a man-in-the-middle attack. DHCP Filtering works by allowing the administrator to configure each port as either a trusted port or an untrusted port. The port that has the authorized DHCP server should be configured as a trusted port. Any DHCP responses received on a trusted port are forwarded. All other ports should be configured as untrusted. Any DHCP (or BootP) responses received are discarded.

From the Services link, you can access the following pages:
- **DHCP Filtering Configuration** on page 72
- **Interface Configuration** on page 73

**DHCP Filtering Configuration**

Use the DHCP Filtering Configuration page to enable or disable the DHCP Filtering feature on the switch.

To access the DHCP Filter Configuration page, click System > Services > DHCP Filtering > Configuration.

To configure global DHCP filtering settings:

1. In the **Admin Mode** field, select **Enable** or **Disable** to turn the DHCP Filtering feature on or off.
2. Click **Apply** to apply the change to the system. The changes take effect immediately.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
Interface Configuration

Use the DHCP Filtering Interface Configuration page to view and configure each port as a trusted or untrusted port. Any DHCP responses received on a trusted port are forwarded. If a port is configured as untrusted, any DHCP (or BootP) responses received on that port are discarded.

To access the DHCP Filtering Interface Configuration page, click System > Services > DHCP Filtering > Interface Configuration.

To configure DHCP filtering settings for an interface:

1. To configure DHCP filtering settings for a physical port, click PORTS.
2. To configure DHCP filtering settings for a Link Aggregation Group (LAG), click LAGS.
3. To configure DHCP filtering settings for both physical ports and LAGs, click ALL.
4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. Choose the trust mode for the selected port(s) or LAG(s).
   - Enable: Any DHCP responses received on this port are forwarded.
   - Disable: Any DHCP (or BootP) responses received on this port are discarded.
6. Click Apply to apply the change to the system. Configuration changes take effect immediately.
7. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
Use the features in the Switching tab to define Layer 2 features. The Switching tab contains links to the following features:

- **Ports** on page 9
- **Link Aggregation Groups** on page 12
- **VLANs** on page 17
- **Voice VLAN** on page 22
- **Auto-VoIP** on page 26
- **Spanning Tree Protocol** on page 27
- **Multicast** on page 41
- **Forwarding Database** on page 54
Ports

The pages on the Ports tab allow you to view and monitor the physical port information for the ports available on the switch. From the Ports link, you can access the following pages:

- *Port Configuration* on page 9
- *Flow Control* on page 11

**Port Configuration**

Use the Port Configuration page to configure the physical interfaces on the switch. To access the Port Configuration page, click **Switching > Ports > Port Configuration**.

![Port Configuration Table](image)

To configure port settings:

1. To configure settings for a physical port, click **PORTS**.
2. To configure settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure settings for both physical ports and LAGs, click **ALL**.
4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. Configure or view the settings:
   - **Description**. Enter the description string to be attached to a port. The string can be up to 64 characters in length.
   - **Port Type**. For most ports this field is blank. Otherwise, the possible values are:
     - **MON**: Indicates that the port is a monitoring port. For additional information about port monitoring see **Port Mirroring** on page 216.
     - **LAG**: Indicates that the port is a member of a Link Aggregation trunk. For more information see **Link Aggregation Groups** on page 12.
   - **Admin Mode**. Use the menu to select the port control administration state, which can be one of the following:
     - **Enable**: The port can participate in the network (default).
     - **Disable**: The port is administratively down and does not participate in the network.
• **Port Speed.** Use the menu to select the port’s speed and duplex mode. If you select Auto, the duplex mode and speed will be set by the auto-negotiation process. The port’s maximum capability (full duplex and 1000 Mbps) will be advertised. Otherwise, your selection will determine the port’s duplex mode and transmission rate. The factory default is Auto.

• **Sleep Mode.** Use the menu to select the port’s Green Ethernet mode, which can be one of the following:
  - Enable: Specifies that when the port link is down, the port automatically goes down for a short amount of time and wakes up to check link pulses. When the port does not have a link partner, the sleep mode reduces power consumption.
  - Disable: The port provides full power to the port even if there is no link partner.

• **Short Cable Mode.** Use the menu to select the port’s Green Ethernet mode, which can be one of the following:
  - Enable: Specifies that cable test is performed when the port link is up at 1 Gbps and if the cable is less than 10m, PHYs are placed in low power mode (nominal power).
  - Disable: The port does not participate in Green Ethernet mode.

• **Physical Status.** Indicates the physical port’s speed and duplex mode

• **Link Status.** Indicates whether the Link is up or down.

• **Link Trap.** This object determines whether or not to send a trap when link status changes. The factory default is Enable.
  - Enable: Specifies that the system sends a trap when the link status changes.
  - Disable: Specifies that the system does not send a trap when the link status changes.

• **Maximum Frame Size.** Specify the maximum Ethernet frame size the interface supports or is configured to support. The frame size includes the Ethernet header, CRC, and payload. (1518–9216). The default maximum frame size is 1518.

• **MAC Address.** Displays the physical address of the specified interface.

• **PortList Bit Offset.** Displays the bit offset value which corresponds to the port when the MIB object type PortList is used to manage in SNMP.

• **ifIndex.** The ifIndex of the interface table entry associated with this port. If the interface field is set to All, this field is blank.

6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

7. If you make any changes to the page, click **Apply** to apply the changes to the system.
Flow Control

IEEE 802.3x flow control works by pausing a port when the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss. When IEEE 802.3x flow control is enabled, lower speed switches can communicate with higher speed switches by requesting that the higher speed switch refrains from sending packets. Transmissions are temporarily halted to prevent buffer overflows.

To display the Flow Control page, click Switching > Ports, and then click the Flow Control link.

To configure global flow control settings:

1. From the Global Flow Control (IEEE 802.3x) Mode field, enable or disable IEEE 802.3x flow control on the system. The factory default is Disable.
   - Enable. The switch sends pause packets if the port buffers become full.
   - Disable. The switch does not send pause packets if the port buffers become full.
2. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
3. If you change the mode, click Apply to apply the changes to the system.
Link Aggregation Groups

Link aggregation groups (LAGs), which are also known as port-channels, allow you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. You assign the LAG VLAN membership after you create a LAG. The LAG by default becomes a member of the management VLAN.

A LAG interface can be either static or dynamic, but not both. All members of a LAG must participate in the same protocols. A static port-channel interface does not require a partner system to be able to aggregate its member ports.

Static LAGs are supported. When a port is added to a LAG as a static member, it neither transmits nor receives LAGPDUs. The GS108T and GS110TP Smart Switches each support four LAGs.

From the LAGs link, you can access the following pages:

- **LAG Configuration** on page 12
- **LAG Membership** on page 14
- **LACP Configuration** on page 15
- **LACP Port Configuration** on page 16

LAG Configuration

Use the LAG (Port Channel) Configuration page to group one or more full-duplex Ethernet links to be aggregated together to form a link aggregation group, which is also known as a port-channel. The switch treats the LAG as if it were a single link.

To access the LAG Configuration page, click **Switching > LAG > Basic > LAG Configuration**.

To configure LAG settings:
1. Select the check box next to the LAG to configure. You can select multiple LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.

2. Configure or view the following settings:
   - **LAG Name.** Specify the name you want assigned to the LAG. You may enter any string of up to 15 alphanumeric characters. A valid name has to be specified in order to create the LAG.
   - **Description.** Specify the Description string to be attached to a LAG. It can be up to 64 characters in length.
   - **LAG ID.** Displays the number assigned to the LAG. This field is read-only.
   - **Link Trap.** Specify whether you want to have a trap sent when link status changes. The factory default is Disable, which will cause the trap to be sent.
   - **Admin Mode.** Select Enable or Disable from the menu. When the LAG (port channel) is disabled, no traffic will flow and LAGPDUs will be dropped, but the links that form the LAG (port channel) will not be released. The factory default is Enable.
   - **STP Mode.** Select the Spanning Tree Protocol Administrative Mode associated with the LAG.
   - **LAG Type.** Select Static or LACP. When the LAG is static, it does not transmit or process received LAGPDUs, for example the member ports do not transmit LAGPDUs and all the LAGPDUs it may receive are dropped. The default is Static.
   - **Active Ports.** A listing of the ports that are actively participating members of this Port Channel. A maximum of 4 ports can be assigned to a port channel.
   - **LAG State.** Indicates whether the link is Up or Down.

3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

4. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
LAG Membership

Use the LAG Membership page to select two or more full-duplex Ethernet links to be aggregated together to form a link aggregation group (LAG), which is also known as a port-channel. The switch can treat the port-channel as if it were a single link.

To access the LAG Membership page, click **Switching > LAG > Basic > LAG Membership**.

To create a LAG:

1. From the **LAG ID** field, select the LAG to configure.
2. In the **LAG Name** field, enter the name you want assigned to the LAG. You may enter any string of up to 15 alphanumeric characters. A valid name has to be specified to create the LAG.
3. Click the orange bar to display the ports.
4. Click the box below each port to include in the LAG. The following figure shows an example of how to configure LAG1 with ports g7 and g8 as members.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
7. To view the ports that are members of the selected LAG, click **Current Members**.
LACP Configuration

To display the LACP Configuration page, click **Switching > LAG > Advanced > LACP Configuration**.

To configure LACP:

1. From the LACP System Priority field, specify the device’s link aggregation priority relative to the devices at the other ends of the links on which link aggregation is enabled. A higher value indicates a lower priority. You can change the value of the parameter globally by specifying a priority from 0–65535. The default value is 32768.
2. Click **Refresh** to reload the page and display the most current information.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
LACP Port Configuration

To display the LACP Port Configuration page, click **Switching > LAG > Advanced > LACP Port Configuration**.

To configure LACP port priority settings:

1. Select the check box next to the port to configure. You can select multiple ports to apply the same setting to all selected ports.

   **Note:** You cannot select ports that are not participating in a LAG.

2. Configure the **LACP Priority** value for the selected port. The field range is 0–255. The default value is 128.

3. Configure the administrative LACP **Timeout** value.
   - **Long.** Specifies a long timeout value.
   - **Short.** Specifies a short timeout value.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

5. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
VLANs

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

By default, all ports on the switch are in the same broadcast domain. VLANs electronically separate ports on the same switch into separate broadcast domains so that broadcast packets are not sent to all the ports on a single switch. When you use a VLAN, users can be grouped by logical function instead of physical location.

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station may omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet may either reject it or insert a tag using its default VLAN ID. A given port may handle traffic for more than one VLAN, but it can only support one default VLAN ID.

From the VLAN link, you can access the following pages:

- VLAN Configuration on page 17
- VLAN Membership Configuration on page 19
- Port VLAN ID Configuration on page 20

VLAN Configuration

Use the VLAN Configuration page to define VLAN groups stored in the VLAN membership table. The GS108T and GS110TP each support up to 64 VLANs. Three VLANs are created by default:

- VLAN 1 is the default VLAN of which all ports are members.
- VLAN 2 is for voice traffic.
- VLAN 3 is for Auto-Video traffic.

To display the VLAN Configuration page, lick Switching > VLAN > Basic > VLAN Configuration.
To configure VLANs:

1. To add a VLAN, configure the VLAN ID, name, and type, and then click **Add**.
   - **VLAN ID**. Specify the VLAN Identifier for the new VLAN. (You can only enter data in this field when you are creating a new VLAN.) The range of the VLAN ID is 1–4093.
   - **VLAN Name**. Use this optional field to specify a name for the VLAN. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 is always named Default.
   - **VLAN Type**. This field identifies the type of the VLAN you are configuring. You cannot change the type of the default VLAN (VLAN ID = 1) because the type is always Default. When you create a VLAN on this page, its type will always be Static.

2. To delete a VLAN, select the check box next to the VLAN ID and click **Delete**. You cannot delete the default VLAN.

3. To modify settings for a VLAN, select the check box next to the VLAN ID, change the desired information, and then click **Apply**. Configuration changes occur immediately.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

5. To reset the VLAN settings on the switch to the factory defaults, select the **Reset Configuration** check box, and click OK in the popup message to confirm. If the Management VLAN is set to a non-default VLAN (VLAN 1), it is automatically set to 1 after a Reset Configuration.
VLAN Membership Configuration

Use this page to configure VLAN Port Membership for a particular VLAN. You can select the Group operation through this page.

To display the VLAN Membership Configuration page, click Switching > VLAN > Advanced > VLAN Membership.

To configure VLAN membership:

1. From the VLAN ID field, select the VLAN to which you want to add ports.
2. Click the orange bar below the VLAN Type field to display the physical ports on the switch.
3. Click the lower orange bar to display the LAGs on the switch.
4. To select the port(s) or LAG(s) to add to the VLAN, click the square below each port or LAG. You can add each interface as a tagged (T) or untagged (U) VLAN member.
   - **Tagged**: Frames transmitted from this port are tagged with the port VLAN ID.
   - **Untagged**: Frames transmitted from this port are untagged. Each port can be an untagged member of only one VLAN. By default, all ports are an untagged member of VLAN 1.

In the following figure, ports g6, g7, and g8 are being added as tagged members to VLAN 2.
5. Use the **Group Operations** field to select all the ports and configure them. Possible values are:
   - **Untag All**: Select all the ports on which all frames transmitted from this VLAN will be untagged. All the ports will be included in the VLAN.
   - **Tag All**: Select the ports on which all frames transmitted for this VLAN will be tagged. All the ports will be included in the VLAN.
   - **Remove All**: This selection has the effect of excluding all ports from the selected VLAN.

6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

7. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

### Port VLAN ID Configuration

The Port PVID Configuration screen lets you assign a port VLAN ID (PVID) to an interface. There are certain requirements for a PVID:

- All ports must have a defined PVID.
- If no other value is specified, the default VLAN PVID is used.
- If you want to change the port’s default PVID, you must first create a VLAN that includes the port as a member.
- Use the Port VLAN ID (PVID) Configuration page to configure a virtual LAN on a port.

To access the Port PVID Configuration page, click **Switching > VLAN > Advanced > Port PVID Configuration**.
To configure PVID information:

1. To configure PVID settings for a physical port, click **PORTS**.
2. To configure PVID settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure PVID settings for both physical ports and LAGs, click **ALL**.
4. Select the check box next to the interfaces to configure. You can select multiple interfaces to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. Configure the PVID to assign to untagged or priority tagged frames received on this port.
6. Specify how you want the port to handle untagged and priority tagged frames. Whichever you select, VLAN tagged frames will be forwarded in accordance with the IEEE 802.1Q VLAN standard. The factory default is **Admit All**.
   - **VLAN Only**: The port will discard any untagged or priority tagged frames it receives.
   - **Admit All**: Untagged and priority tagged frames received on the port will be accepted and assigned the value of the Port VLAN ID for this port.
7. Specify how you want the port to handle tagged frames:
   - **Enable**: A tagged frame will be discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame.
   - **Disable**: All frames are forwarded in accordance with the IEEE 802.1Q VLAN standard. The factory default is Disable.
8. Specify the default 802.1p priority assigned to untagged packets arriving at the port. Possible values are 0–7.
9. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
10. If you make any changes to this page, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.
Voice VLAN

Configure the Voice VLAN settings for ports that carry traffic from IP phones. The Voice VLAN feature can help ensure that the sound quality of an IP phone is safeguarded from deteriorating when the data traffic on the port is high.

From the VLAN link, you can access the following pages:

- Voice VLAN Properties on page 22
- Voice VLAN Port Setting on page 23
- Voice VLAN OUI on page 24

Voice VLAN Properties

To display the Voice VLAN Properties page, click Switching > Voice VLAN > Basic > Properties.

To configure Voice VLAN:

1. From the Voice VLAN Status field, enable or disable Voice VLAN on the switch. If the switch does not handle traffic from IP phones, the status should be disabled.

2. From the Voice VLAN ID field, select the VLAN to use for voice traffic on the switch. The VLAN must already exist on the switch. For information about how to create VLANs, see VLAN Configuration on page 17.

3. From the Class of Service field, set the CoS tag value to be reassigned for packets received on the Voice VLAN when Remark CoS is enabled.

4. From the Remark CoS field, select Enable or Disable to reassign the CoS tag value to packets received on the Voice VLAN.

5. From the Voice VLAN Aging Time field, specify the amount of time after the last IP phone’s OUI is aged out for a specific port. The port will age out after the bridge and voice aging time.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

7. If you make any changes to this page, click **Apply** to send the updated configuration to the switch.

**Voice VLAN Port Setting**

To display the Voice VLAN Port Setting page, click **Switching > Voice VLAN > Advanced > Port Setting**.

To configure Voice VLAN port settings:

1. Select the check box next to the port to configure. You can select multiple check boxes to apply the same setting to all selected ports.

2. From the Voice VLAN Mode menu, specify whether to enable or disable Voice VLAN on the selected port.

3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

4. If you make any changes to this page, click **Apply** to send the updated configuration to the switch.

**Note:** The **Membership** field displays whether the current operational status of the voice VLAN on the interface is active or not active.
Voice VLAN OUI

The Organizational Unique Identifier (OUI) identifies the IP phone manufacturer. The switch comes preconfigured with the following OUIs:

- 00:01:E3: SIEMENS
- 00:03:6B: CISCO1
- 00:12:43: CISCO2
- 00:0F:E2: H3C
- 00:60:B9: NITSUKO
- 00:D0:1E: PINTEL
- 00:E0:75: VERILINK
- 00:E0:BB: 3COM
- 00:04:0D: AVAYA1
- 00:1B:4F: AVAYA2

You can select an existing OUI or add a new OUI and description to identify the IP phones on the network.

To display the Voice VLAN OUI page, click **Switching > Voice VLAN > Advanced > OUI**.

To configure OUI settings:

1. To add a new OUI prefix, type the VOIP OUI prefix in the **Telephony OUI(s)** field, provide a description of the prefix, and click **Add**. The OUI prefix must be in the format AA:BB:CC.
2. To delete an OUI prefix from the list, select the check box next to the OUI prefix and click **Delete**.
3. To modify information for an entry in the OUI list, select the check box next to the OUI prefix, update the OUI prefix or description, and then click **Apply**.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

5. Click **Restore Defaults** to restore the list to the preconfigured OUIs.
Auto-VoIP

The Auto-VoIP automatically makes sure that time-sensitive voice traffic is given priority over data traffic on ports that have this feature enabled. Auto-VoIP checks for packets carrying the following VoIP protocols:

- Session Initiation Protocol (SIP)
- H.323
- Signalling Connection Control Part (SCCP)
- Media Gateway Control Protocol (MGCP)

VoIP frames that are received on ports that have the Auto-VoIP feature enabled are marked with CoS traffic class 3.

To display the Auto-VoIP page, click **Switching > Auto-VoIP**.

To configure Auto-VoIP settings:

1. Select the check box next to the port to configure. You can select multiple check boxes to apply the same setting to all selected ports.
2. From the Auto-VoIP Mode menu, specify whether to enable or disable Auto-VoIP on the selected port.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
4. If you make any changes to this page, click **Apply** to send the updated configuration to the switch.
Spanning Tree Protocol

The Spanning Tree Protocol (STP) provides a tree topology for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops. Spanning tree versions supported include Common STP, Multiple STP, and Rapid STP.

Classic STP provides a single path between end stations, avoiding and eliminating loops. For information on configuring Common STP, see CST Port Configuration on page 31.

Multiple Spanning Tree Protocol (MSTP) supports multiple instances of Spanning Tree to efficiently channel VLAN traffic over different interfaces. Each instance of the Spanning Tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree (RSTP), with slight modifications in the working but not the end effect (chief among the effects, is the rapid transitioning of the port to ‘Forwarding’). The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full-duplex connectivity and ports which are connected to end stations, resulting in rapid transitioning of the port to ‘Forwarding’ state and the suppression of Topology Change Notification. These features are represented by the parameters ‘pointtopoint’ and ‘edgeport’. MSTP is compatible to both RSTP and STP. It behaves appropriately to STP and RSTP bridges. A MSTP bridge can be configured to behave entirely as a RSTP bridge or a STP bridge.

---

**Note:** For two bridges to be in the same region, the force version should be 802.1s and their configuration name, digest key, and revision level should match. For additional information about regions and their effect on network topology, refer to the IEEE 802.1Q standard.

---

The Spanning Tree folder contains links to the following features:

- **STP Switch Configuration** on page 28
- **CST Configuration** on page 30
- **CST Port Configuration** on page 31
- **CST Port Status** on page 33
- **Rapid STP** on page 34
- **MST Configuration** on page 35
- **MST Port Configuration** on page 37
- **STP Statistics** on page 39
STP Switch Configuration

The Spanning Tree Switch Configuration/Status page contains fields for enabling STP on the switch.

To display the Spanning Tree Switch Configuration/Status page, click **Switching > STP > Basic > STP Configuration**.

To configure STP settings on the switch:

1. From the **Spanning Tree State** field, specify whether to enable or disable Spanning Tree operation on the switch.

2. From the **STP Operation Mode** field, specifies the Force Protocol Version parameter for the switch. Options are:
   - **STP** (Spanning Tree Protocol): IEEE 802.1D
   - **RSTP** (Rapid Spanning Tree Protocol): IEEE 802.1w
   - **MSTP** (Multiple Spanning Tree Protocol): IEEE 802.1s

3. Specify the configuration name and revision level.
   - **Configuration Name**. Name used to identify the configuration currently being used. It may be up to 32 alphanumeric characters.
   - **Configuration Revision Level**. Number used to identify the configuration currently being used. The values allowed are between 0 and 65535. The default value is 0.

4. Specify the BPDU Flooding status for all ports or for individual ports. When this feature is enabled, BPDU packets arriving at this port are flooded to other ports if STP is disabled.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

6. If you make any configuration changes, click **Apply** to send the updated configuration to the switch. Configuration changes occur immediately.

The following table describes the STP Status information displayed on the screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge Identifier</td>
<td>The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.</td>
</tr>
<tr>
<td>Time Since Topology Change</td>
<td>The time in seconds since the topology of the CST last changed.</td>
</tr>
<tr>
<td>Topology Change Count</td>
<td>The number of times the topology has changed for the CST.</td>
</tr>
<tr>
<td>Topology Change</td>
<td>The value of the topology change parameter for the switch indicating if a topology change is in progress on any port assigned to the CST. The value is either True or False.</td>
</tr>
<tr>
<td>Designated Root</td>
<td>The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.</td>
</tr>
<tr>
<td>Root Path Cost</td>
<td>Path cost to the Designated Root for the CST.</td>
</tr>
<tr>
<td>Root Port</td>
<td>Port to access the Designated Root for the CST.</td>
</tr>
<tr>
<td>Max Age (secs)</td>
<td>Specifies the bridge maximum age for CST. The value must be less than or equal to (2 X Bridge Forward Delay) – 1 and greater than or equal to 2 X (Bridge Hello Time +1).</td>
</tr>
<tr>
<td>Forward Delay (secs)</td>
<td>Derived value of the Root Port Bridge Forward Delay parameter.</td>
</tr>
<tr>
<td>Hold Time (secs)</td>
<td>Minimum time between transmission of Configuration BPDUs.</td>
</tr>
<tr>
<td>CST Regional Root</td>
<td>Priority and base MAC address of the CST Regional Root.</td>
</tr>
<tr>
<td>CST Path Cost</td>
<td>Path Cost to the CST tree Regional Root.</td>
</tr>
</tbody>
</table>

Click **Refresh** to update the information on the screen with the most current data.
CST Configuration

Use the Spanning Tree CST Configuration page to configure Common Spanning Tree (CST) and Internal Spanning Tree on the switch.

To display the Spanning Tree CST Configuration page, click Switching > STP > Advanced > CST Configuration.

To configure CST settings:

1. Specify values for CST in the appropriate fields:
   - **Bridge Priority.** When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. Specifies the bridge priority value for the Common and Internal Spanning Tree (CST). The valid range is 0–61440. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if the priority is attempted to be set to any value between 0 and 4095, it will be set to 0. The default priority is 32768.
   - **Bridge Max Age (secs).** Specifies the bridge maximum age time for the Common and Internal Spanning Tree (CST), which indicates the amount of time in seconds a bridge waits before implementing a topological change. The valid range is 6–40, and the value must be less than or equal to (2 * Bridge Forward Delay) – 1 and greater than or equal to 2 * (Bridge Hello Time +1). The default value is 20.
   - **Bridge Hello Time (secs).** Specifies the switch Hello time for the Common and Internal Spanning Tree (CST), which indicates the amount of time in seconds a root bridge waits between configuration messages. The value is fixed at 2 seconds.
   - **Bridge Forward Delay (secs).** Specifies the switch forward delay time, which indicates the amount of time in seconds a bridge remains in a listening and learning
state before forwarding packets. The value must be greater or equal to \((\text{Bridge Max Age} / 2) + 1\). The time range is from 4 seconds to 30 seconds. The default value is 15.

- **Spanning Tree Maximum Hops.** Specifies the maximum number of bridge hops the information for a particular CST instance can travel before being discarded. The valid range is 1–127.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

3. If you make any configuration changes, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

The following table describes the MSTP status information displayed on the Spanning Tree CST Configuration page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MST ID</td>
<td>Table consisting of the MST instances (including the CST) and the corresponding VLAN IDs associated with each of them.</td>
</tr>
<tr>
<td>VID</td>
<td>Table consisting of the VLAN IDs and the corresponding FID associated with each of them</td>
</tr>
<tr>
<td>FID</td>
<td>Table consisting of the FIDs and the corresponding VLAN IDs associated with each of them.</td>
</tr>
</tbody>
</table>

Click **Refresh** to update the information on the screen with the most current data.

**CST Port Configuration**

Use the Spanning Tree CST Port Configuration page to configure Common Spanning Tree (CST) and Internal Spanning Tree on a specific port on the switch.

To display the Spanning Tree CST Port Configuration page, click **Switching > STP > Advanced > CST Port Configuration**.
To configure CST port settings:

1. To configure CST settings for a physical port, click **PORTS**.
2. To configure CST settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure CST settings for both physical ports and LAGs, click **ALL**.
4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. Configure the CST values for the selected port(s) or LAG(s):
   - **STP Status.** Enable or disable the Spanning Tree Protocol Administrative Mode associated with the port or port channel.
   - **Fast Link.** Specifies if the specified port is an Edge Port with the CST. Possible values are Enable or Disable. The default is Disable.
   - **Port State.** The Forwarding state of this port. This field is read-only.
   - **Path Cost.** Set the Path Cost to a new value for the specified port in the common and internal spanning tree. It takes a value in the range of 1–200000000.
   - **Priority.** The priority for a particular port within the CST. The port priority is set in multiples of 16. If you specify a value that is not a multiple of 16, the priority is set to the priority is automatically set to the next lowest priority that is a multiple of 16. For example, if you set a value between 0 and 15, the priority is set to 0. If you specify a number between 16 and 31, the priority is set to 16.
   - **External Port Path Cost.** Set the External Path Cost to a new value for the specified port in the spanning tree. It takes a value in the range of 1–200000000.
   - **Port ID.** The port identifier for the specified port within the CST. It is made up from the port priority and the interface number of the port.
- **Hello Timer**: Specifies the switch Hello time, which indicates the amount of time in seconds a port waits between configuration messages. The value is fixed at 2 seconds.

6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

7. If you make any configuration changes, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

8. Click **Refresh** to update the information on the screen with the most current data.

## CST Port Status

Use the Spanning Tree CST Port Status page to display Common Spanning Tree (CST) and Internal Spanning Tree on a specific port on the switch.

To display the Spanning Tree CST Port Status page, click **Switching > STP > Advanced > CST Port Status**.

The following table describes the CST Status information displayed on the screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Select a physical or port channel interface to configure. The port is associated with the VLAN(s) associated with the CST.</td>
</tr>
<tr>
<td>Port Role</td>
<td>Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: <strong>Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.</strong></td>
</tr>
<tr>
<td>Designated Root</td>
<td>Root Bridge for the CST. It is made up using the bridge priority and the base MAC address of the bridge.</td>
</tr>
</tbody>
</table>
### Designated Cost
Displays cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.

### Designated Bridge
Bridge Identifier of the bridge with the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.

### Designated Port
Port Identifier on the Designated Bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.

### Topology Change Acknowledge
Identifies whether the next BPDU to be transmitted for this port would have the topology change acknowledgement flag set. It is either True or False.

### Edge Port
Indicates whether the port is enabled as an edge port. Possible values are Enabled or Disabled.

### Point-to-point MAC
Derived value of the point-to-point status.

### CST Regional Root
Displays the bridge priority and base MAC address of the CST Regional Root.

### CST Path Cost
Displays the path Cost to the CST tree Regional Root.

### Port Forwarding State
Displays the Forwarding State of this port.

Click **Refresh** to update the information on the screen with the most current data.

## Rapid STP
Use the Rapid STP page to view information about Rapid Spanning Tree (RSTP) port status. To display the Rapid STP page, click **Switching > STP > Advanced > RSTP**.
The following table describes the Rapid STP Status information displayed on the screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The physical or port channel interfaces associated with VLANs associated with the CST.</td>
</tr>
<tr>
<td>Role</td>
<td>Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.</td>
</tr>
<tr>
<td>Mode</td>
<td>Specifies the spanning tree operation mode. Different modes are STP, RSTP, and MSTP.</td>
</tr>
<tr>
<td>Fast Link</td>
<td>Indicates whether the port is enabled as an edge port.</td>
</tr>
<tr>
<td>Status</td>
<td>The Forwarding State of this port.</td>
</tr>
</tbody>
</table>

Click Refresh to update the information on the screen with the most current data.

**MST Configuration**

Use the Spanning Tree MST Configuration page to configure Multiple Spanning Tree (MST) on the switch.

To display the Spanning Tree MST Configuration page, click Switching > STP > Advanced > MST Configuration.

To configure an MST instance:

1. To add an MST instance, configure the MST values and click Add:
   - **MST ID.** Specify the ID of the MST to create. Valid values for this are between 1 and 4094.
   - **Priority.** Specifies the bridge priority value for the MST. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the
lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if the priority is attempted to be set to any value between 0 and 4095, it will be set to 0. The default priority is 32768. The valid range is 0–61440.

- **VLAN ID.** The menu contains all VLANs configured on the switch. Select a VLAN to associate with the MST instance.

2. To delete an MST instance, select the check box next to the instance and click **Delete**.

3. To modify an MST instance, select the check box next to the instance to configure, update the values, and click **Apply**. You can select multiple check boxes to apply the same setting to all selected ports.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

For each configured instance, the information described in the following table displays on the page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge Identifier</td>
<td>The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.</td>
</tr>
<tr>
<td>Time Since Topology Change</td>
<td>Displays the total amount of time since the topology of the selected MST instance last changed. The time is displayed in hour/minute/second format, for example, 5 hours, 10 minutes, and 4 seconds.</td>
</tr>
<tr>
<td>Topology Change Count</td>
<td>Displays the total number of times topology has changed for the selected MST instance.</td>
</tr>
<tr>
<td>Topology Change</td>
<td>Indicates whether a topology change is in progress on any port assigned to the selected MST instance. The possible values are <strong>True</strong> or <strong>False</strong>.</td>
</tr>
<tr>
<td>Designated Root</td>
<td>Displays the bridge identifier of the root bridge, which is made up from the bridge priority and the base MAC address of the bridge.</td>
</tr>
<tr>
<td>Root Path Cost</td>
<td>Displays the path cost to the Designated Root for this MST instance.</td>
</tr>
<tr>
<td>Root Port</td>
<td>Indicates the port to access the Designated Root for this MST instance.</td>
</tr>
</tbody>
</table>
MST Port Configuration

Use the Spanning Tree MST Port Configuration page to configure and display Multiple Spanning Tree (MST) settings on a specific port on the switch.

To display the Spanning Tree MST Port Status page, click **Switching > STP > Advanced > MST Port Configuration**. The following figures show the left and right portions of the Web page.

![MST Port Configuration table](image)

**Note:** If no MST instances have been configured on the switch, the page displays a “No MSTs Available” message and does not display any fields.

To configure MST port settings:

1. To configure MST settings for a physical port, click **PORTS**.
2. To configure MST settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure MST settings for both physical ports and LAGs, click **ALL**.

4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.

5. Configure the MST values for the selected port(s) or LAG(s):
   - **Port Priority.** The priority for a particular port within the selected MST instance. The port priority is set in multiples of 16. If you specify a value that is not a multiple of 16, the priority is set to the next lowest priority that is a multiple of 16. For example, if you set a value between 0 and 15, the priority is set to 0. If you specify a number between 16 and 31, the priority is set to 16. It takes a value in the range of 0–240.
   - **Port Path Cost.** Set the Path Cost to a new value for the specified port in the selected MST instance. It takes a value in the range of 1–200000000.

6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

7. If you make any configuration changes, click **Apply** to send the updated configuration to the switch. Configuration changes take place immediately.

The following table describes the read-only MST port configuration information displayed on the Spanning Tree CST Configuration page:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-calculated Port Path</td>
<td>Displays whether the path cost is automatically calculated (Enabled) or not (Disabled). Path</td>
</tr>
<tr>
<td>Cost</td>
<td>cost is calculated based on the link speed of the port if the configured value for Port Path</td>
</tr>
<tr>
<td>Port ID</td>
<td>Cost is zero.</td>
</tr>
<tr>
<td>Port Up Time Since</td>
<td>Time since the counters were last cleared, displayed in Days, Hours, Minutes, and Seconds.</td>
</tr>
<tr>
<td>Counters Last Cleared</td>
<td></td>
</tr>
<tr>
<td>Port Mode</td>
<td>Spanning Tree Protocol Administrative Mode associated with the port or port channel. Possible</td>
</tr>
<tr>
<td></td>
<td>values are <strong>Enable</strong> or <strong>Disable</strong>.</td>
</tr>
<tr>
<td>Port Forwarding State</td>
<td>Indicates the current STP state of a port. If enabled, the port state determines what forwarding</td>
</tr>
<tr>
<td></td>
<td>action is taken on traffic. Possible port states are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>: STP is currently disabled on the port. The port forwards traffic while learning</td>
</tr>
<tr>
<td></td>
<td>MAC addresses.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Blocking</strong>: The port is currently blocked and cannot be used to forward traffic or learn MAC</td>
</tr>
<tr>
<td></td>
<td>addresses.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Listening</strong>: The port is currently in the listening mode. The port cannot forward traffic</td>
</tr>
<tr>
<td></td>
<td>nor can it learn MAC addresses.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Learning</strong>: The port is currently in the learning mode. The port cannot forward traffic,</td>
</tr>
<tr>
<td></td>
<td>however, it can learn new MAC addresses.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Forwarding</strong>: The port is currently in the forwarding mode. The port can forward traffic and</td>
</tr>
<tr>
<td></td>
<td>learn new MAC addresses.</td>
</tr>
</tbody>
</table>
Click **Refresh** to update the screen with the latest MST information.

## STP Statistics

Use the Spanning Tree Statistics page to view information about the number and type of bridge protocol data units (BPDUs) transmitted and received on each port.

To display the Spanning Tree Statistics page, click **Switching > STP > Advanced > STP Statistics**.
The following table describes the information available on the STP Statistics page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Select a physical or port channel interface to view its statistics.</td>
</tr>
<tr>
<td>STP BPDUs Received</td>
<td>Number of STP BPDUs received at the selected port.</td>
</tr>
<tr>
<td>STP BPDUs Transmitted</td>
<td>Number of STP BPDUs transmitted from the selected port.</td>
</tr>
<tr>
<td>RSTP BPDUs Received</td>
<td>Number of RSTP BPDUs received at the selected port.</td>
</tr>
<tr>
<td>RSTP BPDUs Transmitted</td>
<td>Number of RSTP BPDUs transmitted from the selected port.</td>
</tr>
<tr>
<td>MSTP BPDUs Received</td>
<td>Number of MSTP BPDUs received at the selected port.</td>
</tr>
<tr>
<td>MSTP BPDUs Transmitted</td>
<td>Number of MSTP BPDUs transmitted from the selected port.</td>
</tr>
</tbody>
</table>

Click **Refresh** to update the screen with the latest STP statistics information.
Multicast

Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255.

From the Multicast link, you can access the following pages:

- **Auto-Video Configuration** on page 41
- **IGMP Snooping** on page 42
- **IGMP Snooping Querier** on page 50

Auto-Video Configuration

The Auto-Video feature simplifies IGMP Snooping Querier configuration if the switch supports devices or applications running multicast traffic, such as video surveillance cameras.

To access the Auto-Video Configuration page, click **Switching > Multicast > Auto-Video**.

To configure the Auto-Video feature:

1. Enable or disable the Auto-Video feature.
   - **Enable**. The IGMP Snooping Querier is automatically configured with the default VLAN ID for the Auto-Video VLAN
   - **Disable**. IGMP Snooping settings must be manually configured.
2. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch
IGMP Snooping

Internet Group Management Protocol (IGMP) Snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch. Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

A traditional Ethernet network may be separated into different network segments to prevent placing too many devices onto the same shared media. Bridges and switches connect these segments. When a packet with a broadcast or multicast destination address is received, the switch will forward a copy into each of the remaining network segments in accordance with the IEEE MAC Bridge standard. Eventually, the packet is made accessible to all nodes connected to the network.

This approach works well for broadcast packets that are intended to be seen or processed by all connected nodes. In the case of multicast packets, however, this approach could lead to less efficient use of network bandwidth, particularly when the packet is intended for only a small number of nodes. Packets will be flooded into network segments where no node has any interest in receiving the packet. While nodes will rarely incur any processing overhead to filter packets addressed to unrequested group addresses, they are unable to transmit new packets onto the shared media for the period of time that the multicast packet is flooded. The problem of wasting bandwidth is even worse when the LAN segment is not shared, for example in full-duplex links.

Allowing switches to snoop IGMP packets is a creative effort to solve this problem. The switch uses the information in the IGMP packets as they are being forwarded throughout the network to determine which segments should receive packets directed to the group address.

IGMP Snooping Configuration

Use the IGMP Snooping Configuration page to configure the parameters for IGMP snooping, which is used to build forwarding lists for multicast traffic.

To access the IGMP Snooping Configuration page, click Switching > Multicast > IGMP Snooping > IGMP Snooping Configuration.
To configure IGMP Snooping:

1. Enable or disable IGMP Snooping on the switch.
   - **Enable**. The switch snoops all IGMP packets it receives to determine which segments should receive packets directed to the group address.
   - **Disable**. The switch does not snoop IGMP packets.

2. Enable or disable the validation of IGMP IP headers.
   - **Enable**. The switch checks the IGMP IP header for valid Router Alert option, ToS, and TTL information.
   - **Disable**. The switch does not check the IGMP IP header for Router Alert option, ToS, and TTL information.

3. Specify whether to block unknown multicast addresses
   - **Enable**. The switch drops all packets with an unknown multicast MAC address in the destination field.
   - **Disable**. The switch forwards multicast packets with an unknown multicast MAC address in the destination field.

4. Click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
The following table displays information about the global IGMP snooping status and statistics on the page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast Control Frame Count</td>
<td>Displays the number of multicast control frames that have been processed by the CPU.</td>
</tr>
<tr>
<td>Interfaces Enabled for IGMP Snooping</td>
<td>Lists the interfaces currently enabled for IGMP Snooping. To enable interfaces for IGMP snooping, see IGMP Snooping Interface Configuration on page 44.</td>
</tr>
<tr>
<td>Data Frames Forwarded by the CPU</td>
<td>Displays the number of data frames forwarded by the CPU.</td>
</tr>
<tr>
<td>VLAN Ids Enabled For IGMP Snooping</td>
<td>Displays VLAN IDs enabled for IGMP snooping. To enable VLANs for IGMP snooping, see IGMP Snooping VLAN Configuration on page 49.</td>
</tr>
<tr>
<td>VLAN Ids Enabled For IGMP Snooping Querier</td>
<td>Displays VLAN IDs enabled for IGMP snooping querier.</td>
</tr>
</tbody>
</table>

**IGMP Snooping Interface Configuration**

Use the IGMP Snooping Interface Configuration page to configure IGMP snooping settings on specific interfaces.

To access the IGMP Snooping Interface Configuration page, click **Switching > Multicast > IGMP Snooping > IGMP Snooping Interface Configuration**.
To configure IGMP Snooping interface settings:

1. To configure IGMP Snooping settings for a physical port, click PORTS.
2. To configure IGMP Snooping settings for a Link Aggregation Group (LAG), click LAGS.
3. To configure IGMP Snooping settings for both physical ports and LAGs, click ALL.
4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. Configure the IGMP Snooping values for the selected port(s) or LAG(s):
   - **Admin Mode.** Select the interface mode for the selected interface for IGMP Snooping for the switch from the menu. The default is Disable.
   - **Host Timeout.** Specify the amount of time you want the switch to wait for a report for a particular group on a particular interface before it deletes that interface from the group. Enter a value between 2 and 3600 seconds. The default is 260 seconds.
   - **Max Response Time.** Specify the amount of time you want the switch to wait after sending a query on an interface because it did not receive a report for a particular group on that interface. Enter a value greater or equal to 1 and less than the Host Timeout, in seconds. The default is 10 seconds.
   - **MRouter Timeout.** Specify the amount of time you want the switch to wait to receive a query on an interface before removing it from the list of interfaces with multicast routers attached. Enter a value between 0 and 3600 seconds. The default is 0 seconds. A value of zero indicates an infinite timeout; no expiration.
   - **Fast Leave Admin Mode.** Select the Fast Leave mode for a particular interface from the menu. The default is Disable.
6. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
7. If you make any configuration changes, click Apply to apply the new settings to the switch. Configuration changes take effect immediately.

**IGMP Snooping Table**

Use the IGMP Snooping Table page to view all of the entries in the Multicast Forwarding Database that were created for IGMP snooping.

To access the IGMP Snooping Table page, click Switching > Multicast > IGMP Snooping > IGMP Snooping Table.
The following table describes the fields in the IGMP Snooping Table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>A multicast MAC address for which the switch has forwarding and/or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example, 01:00:5e:45:67:89.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>A VLAN ID for which the switch has forwarding and filtering information.</td>
</tr>
<tr>
<td>Type</td>
<td>This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description of this multicast table entry. Possible values are Management Configured, Network Configured, and Network Assisted.</td>
</tr>
<tr>
<td>Interface</td>
<td>The list of interfaces that are designated for forwarding (Fwd) and filtering (Flt) for the associated address.</td>
</tr>
</tbody>
</table>

Use the buttons at the bottom of the page to perform the following actions:

- Click **Clear** to clear one or all of the IGMP Snooping entries.
- Click **Refresh** to reload the page and display the most current information.

### Multicast Forwarding Database Table

The Layer 2 Multicast Forwarding Database (MFDB) is used by the switch to make forwarding decisions for packets that arrive with a multicast destination MAC address. By limiting multicasts to only certain ports in the switch, traffic is prevented from going to parts of the network where that traffic is unnecessary.
When a packet enters the switch, the destination MAC address is combined with the VLAN ID and a search is performed in the Layer 2 Multicast Forwarding Database. If no match is found, then the packet is either flooded to all ports in the VLAN or discarded, depending on the switch configuration. If a match is found, then the packet is forwarded only to the ports that are members of that multicast group.

Use the MFDB Table page to view the port membership information for all active multicast address entries. The key for an entry consists of a MAC address. Entries may contain data for more than one protocol.

To access the MFDB Table page, click Switching > Multicast > IGMP Snooping > MFDB Table.

The following table describes the fields in the MFDB Table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>The MAC Address to which the multicast MAC address is related. To search by MAC address, enter the address with the MFDB table entry you want displayed. Enter six two-digit hexadecimal numbers separated by colons, for example 00:0f:43:67:89:AB, and then click Go. If the address exists, that entry will be displayed. An exact match is required.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID to which the multicast MAC address is related.</td>
</tr>
<tr>
<td>Component</td>
<td>This is the component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping or Static Filtering.</td>
</tr>
<tr>
<td>Type</td>
<td>This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.</td>
</tr>
</tbody>
</table>
Click **Refresh** to update the information on the screen with the most current data.

**MFDB Statistics**

Use the multicast forwarding database Statistics page to view statistical information about the MFDB table.

To access the MFDB Statistics page, click **Switching > Multicast > IGMP Snooping > MFDB Statistics**.
The following table describes the information available on the MFDB Statistics page:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max MFDB Table Entries</td>
<td>Displays the maximum number of entries that the Multicast Forwarding Database table can hold.</td>
</tr>
<tr>
<td>Most MFDB Entries Since</td>
<td>The largest number of entries that have been present in the Multicast Forwarding Database table since the system was last reset. This value is also known as the MFDB high-water mark.</td>
</tr>
<tr>
<td>Last Reset</td>
<td></td>
</tr>
<tr>
<td>Current Entries</td>
<td>Displays the current number of entries in the Multicast Forwarding Database table.</td>
</tr>
</tbody>
</table>

Click **Refresh** to update the information on the screen with the most current data.

**IGMP Snooping VLAN Configuration**

Use the IGMP Snooping VLAN Configuration page to configure IGMP snooping settings for VLANs on the system.

To access the IGMP Snooping VLAN Configuration page, click **Switching > Multicast > IGMP Snooping > IGMP Snooping VLAN Configuration**.

![IGMP Snooping VLAN Configuration](image)

To configure IGMP snooping settings for VLANs:

1. To enable IGMP snooping on a VLAN, enter the VLAN ID in the appropriate field and configure the IGMP Snooping values:

   - **Fast Leave Admin Mode**. Enable or disable the IGMP Snooping Fast Leave Mode for the specified VLAN ID. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface. You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the
inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.

- **Host Timeout.** Sets the value for group membership interval of IGMP snooping for the specified VLAN ID. The valid range is (Maximum Response Time + 1) to 3600 seconds.

- **Maximum Response Time.** Enter the amount of time in seconds that a switch will wait after sending a query on the VLAN because it did not receive a report for a particular group in that interface. value. The valid range is 1 to 25 seconds. Its value must be less than the Host Timeout value.

- **MRouter Timeout.** Enter the amount of time that a switch will wait to receive a query on the VLAN before removing it from the list of VLANs with multicast routers attached. Enter a value between 0 and 3600 seconds. The default is 0 seconds, which means there is no expiration.

- **Query Mode.** Enable or disable the IGMP Querier Mode for the specified VLAN ID.

- **Query Interval.** Enter the value for IGMP Query Interval for the specified VLAN ID. The valid range is 1–1800 seconds. The default is 60 seconds.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

3. To disable IGMP snooping on a VLAN and remove it from the list, select the check box next to the VLAN ID and click **Delete**.

4. To modify IGMP snooping settings for a VLAN, select the check box next to the VLAN ID, update the desired values, and click **Apply**.

5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

**IGMP Snooping Querier**

IGMP snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the IGMP querier. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

These pages enable you to configure and display information on IGMP snooping queriers on the network and, separately, on VLANs.

The IGMP Snooping Querier feature contains links to the following pages:

- **IGMP Snooping Querier Configuration** on page 51
- **IGMP Snooping Querier VLAN Configuration** on page 52
- **IGMP Snooping Querier VLAN Status** on page 53
IGMP Snooping Querier Configuration

Use this page to enable or disable the IGMP Snooping Querier feature, specify the IP address of the router to perform the querying, and configure the related parameters.

To access this page, click Switching > Multicast > IGMP Snooping Querier > IGMP Snooping > Querier Configuration.

To configure IGMP Snooping Querier settings:

1. From the Querier Admin Mode field, enable or disable the administrative mode for IGMP Snooping Querier.
2. In the Snooping Querier Address field, specify the IP address to be used as source address in periodic IGMP queries. This address is used when no address is configured on the VLAN on which the query is being sent.
3. In the IGMP Version field, specify the IGMP protocol version used in periodic IGMP queries.
4. In the Query Interval field, specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1–1800 seconds. The default value is 60.
5. In the Querier Expiry Interval field, specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60–300 seconds. The default value is 60.
6. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
7. Click Apply to apply the new settings to the switch. Configuration changes take effect immediately.
8. Click Refresh to update the page with the latest information from the switch.
**IGMP Snooping Querier VLAN Configuration**

Use this page to configure IGMP queriers for use with VLANs on the network.

To access this page, click **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Configuration**.

To configure Querier VLAN settings:

1. To create a new VLAN ID for IGMP Snooping, select New Entry from the VLAN ID field and complete the following fields:
   - **VLAN ID**. Specifies the VLAN ID for which the IGMP Snooping Querier is to be enabled.
   - **Querier Election Participate Mode**. Enable or disable Querier Participate Mode.
     - **Disabled**. Upon seeing another querier of the same version in the VLAN, the snooping querier moves to the non-querier state.
     - **Enabled**. The snooping querier participates in querier election, in which the least IP address operates as the querier in that VLAN. The other querier moves to non-querier state.
   - **Snooping Querier VLAN Address**. Specify the Snooping Querier IP Address to be used as the source address in periodic IGMP queries sent on the specified VLAN.

2. Click **Apply** to apply the new settings to the switch. Configuration changes take effect immediately.

3. To disable Snooping Querier on a VLAN, select the VLAN ID and click **Delete**.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

5. Click **Refresh** to update the page with the latest information from the switch.
**IGMP Snooping Querier VLAN Status**

Use this page to view the operational state and other information for IGMP snooping queriers for VLANs on the network.

To access this page, click **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Status**.

The following table describes the information available on the Querier VLAN Status page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>Specifies the VLAN ID on which the IGMP Snooping Querier is administratively enabled and for which VLAN exists in the VLAN database.</td>
</tr>
<tr>
<td>Operational State</td>
<td>Specifies the operational state of the IGMP Snooping Querier on a VLAN:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Querier</strong>: The snooping switch is the querier in the VLAN. The snooping switch will send out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch sees a better querier (numerically lower) in the VLAN, it moves to non-querier mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Non-Querier</strong>: The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch moves into querier mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>: The snooping querier is not operational on the VLAN. The snooping querier moves to disabled mode when IGMP snooping is not operational on the VLAN, when the querier address is not configured, or the network management address is not configured.</td>
</tr>
<tr>
<td>Operational Version</td>
<td>Displays the IGMP protocol version of the operational querier.</td>
</tr>
<tr>
<td>Last Querier Address</td>
<td>Displays the IP address of the last querier from which a query was snooped on the VLAN.</td>
</tr>
<tr>
<td>Last Querier Version</td>
<td>Displays the IGMP protocol version of the last querier from which a query was snooped on the VLAN.</td>
</tr>
<tr>
<td>Operational Max Response Time</td>
<td>Displays the maximum response time to be used in the queries that are sent by the snooping querier.</td>
</tr>
</tbody>
</table>

Click **Refresh** to redisplay the page with the latest information from the switch.
Forwarding Database

The forwarding database maintains a list of MAC addresses after having received a packet from this MAC address. The transparent bridging function uses the forwarding database entries to determine how to forward a received frame.

The Address Table folder contains links to the following features:

- **MAC Address Table** on page 54
- **Dynamic Address Configuration** on page 56
- **Static MAC Address** on page 57

MAC Address Table

The MAC Address Table contains information about unicast entries for which the switch has forwarding and/or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame. Use the search function of the MAC Address Table page to display information about the entries in the table.

To access this page, click **Switching > Address Table > Basic > Address Table**.

To search for an entry in the MAC Address Table:

1. Use the Search By field to search for MAC Addresses by **MAC Address**, **VLAN ID**, or **Interface**.
• **MAC Address**: Select **MAC Address** from the menu and enter a six-byte hexadecimal MAC address in two-digit groups separated by colons, then click **Go**. If the address exists, that entry will be displayed. An exact match is required.

• **VLAN ID**: Select **VLAN ID** from the menu, enter the VLAN ID, for example, 100. Then click **Go**. If any entries with that VLAN ID exist they are displayed.

• **Interface**: Select **Interface** from the menu, enter the interface ID in g1, g2... format, then, click **Go**. If any entries learned on that interface exist, they are displayed.

2. Click **Clear** to clear Dynamic MAC Addresses in the table.

3. Click **Refresh** to redisplay the page to show the latest MAC Addresses.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

The following table describes the information available for each entry in the address table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>Specifies the VLAN ID on which the IGMP Snooping Querier is administratively enabled and for which VLAN exists in the VLAN database.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a six-byte MAC address with each byte separated by colons. For example, 00:0F:89:AB:CD:EF.</td>
</tr>
<tr>
<td>Interface</td>
<td>The port where this address was learned; that is, this field displays the port through which the MAC address can be reached.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of this entry. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Static</strong>: The entry was added when a static MAC filter was defined.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Learned</strong>: The entry was learned by observing the source MAC addresses of incoming traffic, and is currently in use.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Management</strong>: The system MAC address, which is identified with interface c1.</td>
</tr>
</tbody>
</table>
Dynamic Address Configuration

Use the Dynamic Addresses page to set the amount of time to keep a learned MAC address entry in the forwarding database. The forwarding database contains static entries, which are never aged out, and dynamically learned entries, which are removed if they are not updated within a given time.

To access the Configuration page, click **Switching > Address Table > Advanced > Dynamic Addresses**.

To configure the Dynamic Address setting:

1. Specify the number of seconds the forwarding database should wait before deleting a learned entry that has not been updated. IEEE 802.1D-1990 recommends a default of 300 seconds. You may enter any number of seconds between 10 and 1000000. The factory default is 300.

   **Note:** IEEE 802.1D recommends a default of 300 seconds, which is the factory default.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

3. Click **Apply** to apply to send the updated configuration to the switch. Configuration changes take effect immediately.
Static MAC Address

Use the Static MAC Address Configuration page to configure and view static MAC addresses on an interface.

To access the Static MAC Address Configuration page, click Switching > Address Table > Advanced > Static MAC Address.

To configure a static MAC address:

1. To add a static MAC address entry
   a. Select the VLAN ID corresponding to the MAC address to add.
   b. Specify the MAC address to add.
   c. Specify the port associated with the MAC address.
   d. Click Add.

2. To delete a static MAC address, select the check box next to the entry and click Delete.

3. To modify the settings for a static MAC address, select the check box next to the entry, update the desired values, and click Apply.

4. Click Refresh to reload the page and display the latest MAC address learned on a specific port.

5. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
Use the features in the QoS tab to configure Quality of Service (QoS) settings on the switch. The QoS tab contains links to the following features:

- *Class of Service* on page 126
- *Differentiated Services* on page 133

In a typical switch, each physical port consists of one or more queues for transmitting packets on the attached network. Multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission. As queues become full, packets have no place to be held for transmission and get dropped by the switch.

QoS is a means of providing consistent, predictable data delivery by distinguishing between packets that have strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given “special treatment” in a QoS-capable network. With this in mind, all elements of the network must be QoS-capable. The presence of at least one node which is not QoS-capable creates a deficiency in the network path and the performance of the entire packet flow is compromised.
Class of Service

The Class of Service (CoS) queueing feature lets you directly configure certain aspects of switch queueing. This provides the desired QoS behavior for different types of network traffic when the complexities of DiffServ are not required. The priority of a packet arriving at an interface can be used to steer the packet to the appropriate outbound CoS queue through a mapping table. CoS queue characteristics that affect queue mapping, such as minimum guaranteed bandwidth, or transmission rate shaping are user-configurable at the queue (or port) level.

Four queues per port are supported.

From the Class of Service link under the QoS tab, you can access the following pages:

- **Basic CoS Configuration** on page 126
- **CoS Interface Configuration** on page 128
- **Interface Queue Configuration** on page 129
- **802.1p to Queue Mapping** on page 130
- **DSCP to Queue Mapping** on page 131

Basic CoS Configuration

Use the Trust Mode Configuration page to set the class of service trust mode of an interface. Each port in the switch can be configured to trust one of the packet fields (802.1p or IP DSCP), or to not trust any packet’s priority designation (untrusted mode). If the port is set to a trusted mode, it uses a mapping table appropriate for the trusted field being used. This mapping table indicates the CoS queue to which the packet should be forwarded on the appropriate egress port(s). Of course, the trusted field must exist in the packet for the mapping table to be of any use, so there are default actions performed when this is not the case. These actions involve directing the packet to a specific CoS level configured for the ingress port as a whole, based on the existing port default priority as mapped to a traffic class by the current 802.1p mapping table.

Alternatively, when a port is configured as untrusted, it does not trust any incoming packet priority designation and uses the port default priority value instead. All packets arriving at the ingress of an untrusted port are directed to a specific CoS queue on the appropriate egress port(s), in accordance with the configured default priority of the ingress port. This process is also used for cases where a trusted port mapping is unable to be honored, such as when a non-IP packet arrives at a port configured to trust the IP DSCP value.

To display the Basic CoS Configuration page, click **QoS > Basic > CoS Configuration**.
To configure global CoS settings:

1. Select the **Global** radio button to configure the trust mode settings that apply to all interfaces.
   
   Alternatively, you can select the **Interface** radio button to apply trust mode settings to individual interfaces. The per-interface setting overrides the global settings.

2. Select the trust mode for all interfaces (**Global Trust Mode**) or the selected interface (**Interface Trust Mode**). This setting determines the type of CoS marking to trust when the frame enters the port.
   - **Untrusted**. Do not trust any CoS packet marking at ingress.
   - **802.1p**. The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of four internal hardware priority queues: High, Normal, Low, and Lowest.
   - **DSCP**. The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.

3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

4. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch.
CoS Interface Configuration

Use the CoS Interface Configuration page to apply an interface shaping rate to all interfaces or to a specific interface.

To display the CoS Interface Configuration page, click the QoS > CoS tab, and then click the Advanced > CoS Interface Configuration link.

To configure CoS settings for an interface:

1. To configure CoS settings for a physical port, click PORTS.
2. To configure CoS settings for a Link Aggregation Group (LAG), click LAGS.
3. To configure CoS settings for both physical ports and LAGs, click ALL.
4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces.
5. From the Interface Trust Mode field, specify whether or not the selected interface(s) trust a particular packet marking when the packet enters the port.
   - Untrusted. Do not trust any CoS packet marking at ingress.
   - 802.1p. The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of four internal hardware priority queues: High, Normal, Low, and Lowest.
   - DSCP. The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.
6. From the **Interface Shaping Rate** field, specify the maximum bandwidth allowed on the selected interface(s). This setting is typically used to shape the outbound transmission rate in increments of 64 kbps. This value is controlled independently of any per-queue maximum bandwidth configuration. It is effectively a second-level shaping mechanism. The default value is 0, in increments of 16. A value of 0 means the maximum is unlimited.

7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

8. If you make changes to the page, click **Apply** to apply the changes to the system.

**Interface Queue Configuration**

Use the Interface Queue Configuration page to define what a particular queue does by configuring switch egress queues. User-configurable parameters control the amount of bandwidth used by the queue, the queue depth during times of congestion, and the scheduling of packet transmission from the set of all queues on a port. Each port has its own CoS queue-related configuration.

The configuration process is simplified by allowing each CoS queue parameter to be configured globally or per-port. A global configuration change is automatically applied to all ports in the system.

To display the Interface Queue Configuration page, click the **QoS > CoS** tab, and then click the **Advanced > Interface Queue Configuration** link.

To configure CoS queue settings for an interface:

1. To configure CoS queue settings for a physical port, click **PORTS**.
2. To configure CoS queue settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure CoS queue settings for both physical ports and LAGs, click **ALL**.

4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply a trust mode or rate to all interfaces.

5. Configure any of the following settings:
   - **Queue ID.** Use the menu to select the queue to be configured.
   - **Minimum Bandwidth.** Enter a percentage of the maximum negotiated bandwidth for the selected queue on the interface. Specify a percentage from 0–100, in increments of 1.
   - **Scheduler Type.** Selects the type of queue processing from the drop down menu. Options are Weighted and Strict. Defining on a per-queue basis allows the user to create the desired service characteristics for different types of traffic.
     - **Weighted:** Weighted round robin associates a weight to each queue. This is the default.
     - **Strict:** Services traffic with the highest priority on a queue first.
   - **Queue Management Type.** Displays the type of packet management used for all packets, which is Taildrop. All packets on a queue are safe until congestion occurs. At this point, any additional packets queued are dropped.

6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

7. If you make changes to the page, click **Apply** to apply the changes to the system.

### 802.1p to Queue Mapping

The 802.1p to Queue Mapping page also displays the Current 802.1p Priority Mapping table. To display the 802.1p to Queue Mapping page, click **QoS > CoS > Advanced > 802.1p to Queue Mapping**.
To map 802.1p priorities to queues:

1. Select the Global radio button to apply the same 802.1p priority mapping to all CoS configurable interfaces or select the Interface radio button to apply 802.1p priority mapping to on a per-interface basis.

   If you map 802.1p priorities to individual interfaces, select the Interface radio button and then select the interface from the drop-down menu. The interface settings override the global settings for 802.1p priority mapping.

2. Select the queue to map to the predefined 802.1p priority values.

   The 802.1p Priority row contains traffic class selectors for each of the eight 802.1p priorities to be mapped. The priority goes from low (0) to high (3). For example, traffic with a priority of 0 is for most data traffic and is sent using “best effort.” Traffic with a higher priority, such as 3, might be time-sensitive traffic, such as voice or video.

   The values in each drop down menu represent the traffic class. The traffic class is the hardware queue for a port. Higher traffic class values indicate a higher queue position. Before traffic in a lower queue is sent, it must wait for traffic in higher queues to be sent.

3. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

4. If you make changes to the page, click Apply to apply the changes to the system.

DSCP to Queue Mapping

Use the DSCP to Queue Mapping page to specify which internal traffic class to map the corresponding DSCP value.

To display the IP DSCP Mapping page, click QoS > CoS > Advanced > DSCP to Queue Mapping.
To map DSCP values to queues:

1. For each DSCP value, select a hardware queue to associate with the value.
   
   The traffic class is the hardware queue for a port. Higher traffic class values indicate a higher queue position. Before traffic in a lower queue is sent, it must wait for traffic in higher queues to be sent. Valid range is 0–3.

2. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

3. If you make changes to the page, click Apply to apply the changes to the system.
Differentiated Services

The QoS feature contains Differentiated Services (DiffServ) support that allows traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors.

Standard IP-based networks are designed to provide “best effort” data delivery service. “Best effort” service implies that the network delivers the data in a timely fashion, although there is no guarantee that it will. During times of congestion, packets may be delayed, sent sporadically, or dropped. For typical Internet applications, such as e-mail and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. Conversely, any degradation of service has undesirable effects on applications with strict timing requirements, such as voice or multimedia.

Defining DiffServ

To use DiffServ for QoS, the Web pages accessible from the Differentiated Services menu page must first be used to define the following categories and their criteria:

1. Class: Create classes and define class criteria.
2. Policy: Create policies, associate classes with policies, and define policy statements.
3. Service: Add a policy to an inbound interface

Packets are classified and processed based on defined criteria. The classification criteria is defined by a class. The processing is defined by a policy’s attributes. Policy attributes may be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs. A policy can contain multiples classes. When the policy is active, the actions taken depend on which class matches the packet.

Packet processing begins by testing the class match criteria for a packet. A policy is applied to a packet when a class match within that policy is found.

The Differentiated Services menu page contains links to the various DiffServ configuration and display features.

To display the page, click QoS > DiffServ. The Differentiated Services menu page contains links to the following features:

- DiffServ Configuration
- Class Configuration
- Policy Configuration
- Service Configuration
- Service Statistics
Diffserv Configuration

Use the Diffserv Configuration page to display DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables.

To display the page, click QoS > DiffServ > Advanced > Diffserv Configuration.

To configure the global Diffserv mode:

1. Select the administrative mode for DiffServ:
   - Enable. Differentiated Services are active.
   - Disable. The DiffServ configuration is retained and can be changed, but it is not active.

2. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

3. If you make changes to the page, click Apply to apply the changes to the system.

The following table describes the information displayed in the Status table on the DiffServ Configuration page:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Table</td>
<td>Displays the current and maximum number of rows of the class table.</td>
</tr>
<tr>
<td>Class Rule Table</td>
<td>Displays the current and maximum number of rows of the class rule table.</td>
</tr>
<tr>
<td>Policy Table</td>
<td>Displays the current and maximum number of rows of the policy table.</td>
</tr>
</tbody>
</table>
Click **Refresh** to update the page with the current settings.

## Class Configuration

Use the Class Configuration page to add a new DiffServ class name, or to rename or delete an existing class. The page also allows you to define the criteria to associate with a DiffServ class. As packets are received, these DiffServ classes are used to prioritize packets. You can have multiple match criteria in a class. The logic is a Boolean logical-and for this criteria. After creating a Class, click the class link to the Class page.

To display the page, click **QoS > DiffServ > Advanced > Class Configuration**.

### To configure a DiffServ class:

1. To create a new class, enter a class name, select the class type, and click **Add**.
   
   The switch supports only the Class Type value All, which means all the various match criteria defined for the class should be satisfied for a packet match. All signifies the logical AND of all the match criteria.

2. To rename an existing class, select the check box next to the configured class, update the name, and click **Apply**.

3. To remove a class, click the check box beside the Class Name, then click **Delete**.

4. Click **Refresh** to refresh the page with the most current data from the switch.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch. After creating a Class, click the class link to the Class page.

To configure the class match criteria:

1. Click the class name for an existing class.

The class name is a hyperlink. The following figure shows the configuration fields for the class.
2. Define the criteria to associate with a DiffServ class:

- **Reference Class.** Selects a class to start referencing for criteria. A specified class can reference at most one other class of the same type.

- **Class of Service.** Select the field and enter a class of service 802.1p user priority value to be matched for the packets. The valid range is 0–7.

- **VLAN.** Select the field and enter a VLAN ID to be matched for packets. The VLAN ID range is 1–4093.

- **EtherType.** Select the EtherType field to compare the match criteria against the value in the header of an Ethernet frame. Select an EtherType keyword or enter an EtherType value to specify the match criteria. If you specify the EtherType value, select User Value from the menu and enter a custom protocol identifier to which packets are matched. The value is a four-digit hexadecimal number in the range of 0600–FFFF.

- **Source MAC.** Select this field and enter the source MAC address to compare against an Ethernet frame.

- **Source MAC Mask.** Enter the source MAC address mask specifying which bits in the destination MAC to compare against an Ethernet frame. An f indicates that the address bit is significant, and an 0 indicates that the address bit is to be ignored. A MAC mask of ff:ff:ff:ff:ff:ff matches a single MAC address.

- **Destination MAC.** Select this field and enter the destination MAC address to compare against an Ethernet frame.

- **Destination MAC Mask.** Enter the destination MAC address mask specifying which bits in the destination MAC to compare against an Ethernet frame. An f indicates that the address bit is significant, and an 0 indicates that the address bit is to be ignored. A MAC mask of ff:ff:ff:ff:ff:ff matches a single MAC address.

- **Protocol Type.** Requires a packet's layer 4 protocol to match the protocol you select. If you select Other, enter a protocol number in the field that appears. The valid range is 0–255.

- **Source IP Address.** Requires a packet's source port IP address to match the address listed here. In the IP Address field, enter a valid source IP address in dotted decimal format.

- **Source Mask.** Enter a valid subnet mask to determine which bits in the IP address are significant. Note that this is not a wildcard mask.

- **Source L4 Port.** Requires a packet's TCP/UDP source port to match the port you select. Select the desired L4 keyword from the list on which the rule can be based. If you select Other, the screen refreshes and a Port ID field appears. Enter a user-defined Port ID by which packets are matched to the rule.

- **Destination IP Address.** Requires a packet's destination port IP address to match the address listed here. In the IP Address field, enter a valid destination IP address in dotted decimal format.

- **Destination Mask.** Enter a valid subnet mask to determine which bits in the IP address are significant. This is not a wildcard mask.

- **Destination L4 Port.** Requires a packet's TCP/UDP destination port to match the port you select. Select the desired L4 keyword from the list on which the rule can be
based. If you select Other, the screen refreshes and a Port ID field appears. Enter a user-defined Port ID by which packets are matched to the rule.

- **IP DSCP.** Matches the packet’s DSCP to the class criteria’s when selected. Select the DSCP type from the menu or enter a DSCP value to match. If you select Other, enter a custom value in the DSCP Value field that appears.

- **IP Precedence.** Matches the packet’s IP Precedence value to the class criteria’s when Enter a value in the range of 0–7.

- **IP ToS.** Matches the packet’s Type of Service bits in the IP header to the class criteria’s when selected and a value is entered. In the ToS Bits field, enter a two-digit hexadecimal number to match the bits in a packet’s ToS field. In the ToS Mask field, specify the bit positions that are used for comparison against the IP ToS field in a packet.

3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

4. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes occur immediately.

5. Click **Refresh** to refresh the page with the most current data from the switch.

### Policy Configuration

Use the Policy Configuration page to associate a collection of classes with one or more policy statements. After creating a Policy, click the policy link to the Policy page.

To display the page, click **QoS > DiffServ > Advanced > Policy Configuration.**

![Policy Configuration Page](image)

To configure a DiffServ policy:

1. To create a new policy, enter a policy name in the Policy Selector field, select the existing DiffServ class to associate with the policy, and click **Add.**
The available policy type is In, which indicates the type is specific to inbound traffic. This field is not configurable.

2. To rename an existing policy or add a new member class to the policy, select the check box next to the configured class, update the fields, and click **Apply**.

3. To remove a policy, click the check box beside the policy, then click **Delete**.

4. Click **Refresh** to refresh the page with the most current data from the switch.

5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch. After creating a Class, click the class link to the Class page.

To configure the policy attributes:

1. Click the name of the policy.
The policy name is a hyperlink. The following figure shows the configuration fields for the policy.

2. Select the queue to which packets will of this policy-class will be assigned.

3. Configure the policy attributes:
   - **Drop**. Select this option to drop packets for this policy-class.
   - **Mark CoS**. Enter the specified Class of Service queue number to mark all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header. If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0–7.
   - **Mark IP Precedence**. Use this attribute to mark all packets for the associated traffic stream with the IP Precedence value you enter in the IP Precedence Value field.
   - **Mark IP DSCP**. Use this attribute to mark all packets for the associated traffic stream with IP DSCP value you choose from the menu.
• **Simple Policy.** Use this attribute to establish the traffic policing style for the specified class. The simple form of the policy command uses a single data rate and burst size, resulting in two outcomes: confirm and violate.

4. If you select the Simple Policy attribute, you can configure the following fields:

- **Color Mode.** Color Aware mode requires the existence of one or more color classes that are valid for use with this policy instance; otherwise, the color mode is color blind, which is the default.

- **Color Conform Class.** A valid color class contains a single, non-excluded match criterion for one of the following fields (provided the field does not conflict with the classifier of the policy instance itself).

- **Color Conform Mode.** The match-criteria of the color Conform class.

- **Committed Rate.** The committed rate is specified in kilobits-per-second (Kbps) and is an integer from 1–4294967295.

- **Committed Burst Size.** The committed burst size is specified in kilobytes (KB) and is an integer from 1–128.

- **Conform Action.** Determines what happens to packets that are considered conforming (below the police rate). Select one of the following actions:
  - **Send.** (default) These packets are presented unmodified by DiffServ to the system forwarding element.
  - **Drop.** These packets are immediately dropped.
  - **Mark CoS.** These packets are marked by DiffServ with the specified CoS value before being presented to the system forwarding element. This selection requires that the Mark CoS value field be set.
  - **Mark IP Precedence.** These packets are marked by DiffServ with the specified IP Precedence value before being presented to the system forwarding element. This selection requires that the Mark IP Precedence value field be set.
  - **Mark IP DSCP.** These packets are marked by DiffServ with the specified DSCP value before being presented to the system forwarding element. This selection requires that the DSCP value field be set.

- **Violate Action.** Determines what happens to packets that are considered non-conforming (above the police rate). Select one of the following actions:
  - **Send.** (default) These packets are presented unmodified by DiffServ to the system forwarding element.
  - **Drop.** (default) These packets are immediately dropped.
  - **Mark CoS.** These packets are marked by DiffServ with the specified CoS value before being presented to the system forwarding element. This selection requires that the Mark CoS value field be set.
  - **Mark IP Precedence.** These packets are marked by DiffServ with the specified IP Precedence value before being presented to the system forwarding element. This selection requires that the Mark IP Precedence value field be set.
  - **Mark IP DSCP.** These packets are marked by DiffServ with the specified DSCP value before being presented to the system forwarding element. This selection requires that the DSCP value field be set.
5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

6. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

7. Click **Refresh** to refresh the page with the most current data from the switch.

**Service Configuration**

Use the Service Configuration page to activate a policy on an interface.

To display the page, click **QoS** > **DiffServ** > **Advanced** > **Service Configuration**.

To configure DiffServ policy settings on an interface:

1. To configure DiffServ policy settings for a physical port, click **PORTS**.
2. To configure DiffServ policy settings for a Link Aggregation Group (LAG), click **LAGS**.
3. To configure DiffServ policy settings for both physical ports and LAGs, click **ALL**.
4. Select the check box next to the port or LAG to configure. You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. To activate a policy for the selected interface(s) select the policy from the **Policy In** menu, and then click **Apply**.
6. To remove a policy from the selected interface(s) select None from the **Policy In** menu, and then click **Apply**.
7. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
Service Statistics

Use the Service Statistics page to display service-level statistical information about all interfaces that have DiffServ policies attached.

To display the page, click the QoS > DiffServ tab and then click the Advanced > Service Statistics link.

The following table describes the information available on the Service Statistics page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Displays the interface for which service statistics are to display.</td>
</tr>
<tr>
<td>Direction</td>
<td>Displays the direction of packets for which service statistics display, which is always In.</td>
</tr>
<tr>
<td>Policy Name</td>
<td>Displays the policy associated with the selected interface.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Displays the operational status of this service interface, which is either Up or Down.</td>
</tr>
<tr>
<td>Discarded Packets</td>
<td>Displays the total number of packets discarded for all class instances in this service policy for any reason due to DiffServ treatment. This is the overall count per-interface, per-direction.</td>
</tr>
<tr>
<td>Member Classes</td>
<td>Selects the member class for which octet statistics are to display.</td>
</tr>
</tbody>
</table>

Click Refresh to update the page with the most current information.
Managing Device Security

Use the features available from the Security tab to configure management security settings for port, user, and server security. The Security tab contains links to the following features:

- Management Security Settings on page 146
- Configuring Management Access on page 157
- Port Authentication on page 164
- Traffic Control on page 171
- Configuring Access Control Lists on page 180
Management Security Settings

From the Management Security Settings page, you can configure the login password, Remote Authorization Dial-In User Service (RADIUS) settings, Terminal Access Controller Access Control System (TACACS+) settings, and authentication lists.

To display the page, click the Security > Management Security tab. The Management Security folder contains links to the following features:

- Change Password on page 146
- RADIUS Configuration on page 147
- Configuring TACACS+ on page 153
- Authentication List Configuration on page 155

Change Password

Use the page to change the login password. To display the page, click Security > Management Security > User Configuration > Change Password.

To change the login password for the management interface:

1. Specify the current password in the Old Password. The entered password will be displayed in asterisks (*). Passwords are 1–20 alphanumeric characters in length and are case sensitive.

2. Enter the new password. It will not display as it is typed, and only asterisks (*) will show on the screen. Passwords are 1–20 alphanumeric characters in length and are case sensitive.

3. To confirm the password, enter it again to make sure you entered it correctly. This field will not display, but will show asterisks (*).

4. Use the Reset Password field to reset the password to the default value.

5. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. If you make changes to the page, click **Apply** to apply the changes to the system.

---

**Note:** In the case of a lost password, press the Factory Default Reset button on the front panel for more than one second to restore the factory default. The reset button will only reboot the device.

---

### RADIUS Configuration

RADIUS servers provide additional security for networks. The RADIUS server maintains a user database, which contains per-user authentication information. The switch passes information to the configured RADIUS server, which can authenticate a user name and password before authorizing use of the network. RADIUS servers provide a centralized authentication method for:

- Web Access
- Access Control Port (802.1X)

The RADIUS folder contains links to the following features:

- **Global Configuration** on page 147
- **RADIUS Server Configuration** on page 148
- **Accounting Server Configuration** on page 150

### Global Configuration

Use the RADIUS Configuration page to add information about one or more RADIUS servers on the network.

To access the RADIUS **Configuration** page, click **Security > Management Security > RADIUS > Global Configuration**.

![RADIUS Configuration Page](image)
The Current Server IP Address field is blank if no servers are configured (see *RADIUS Server Configuration* on page 148). The switch supports up to three configured RADIUS servers. If more than one RADIUS servers are configured, the current server is the server configured as the primary server. If no servers are configured as the primary server, the current server is the most recently added RADIUS server.

To configure global RADIUS server settings:

1. In the **Max Number of Retransmits** field, specify the value of the maximum number of times a request packet is retransmitted to the RADIUS server.

   Consideration to maximum delay time should be given when configuring RADIUS max retransmit and RADIUS timeout. If multiple RADIUS servers are configured, the max retransmit value on each will be exhausted before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the sum of (retransmit times timeout) for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.

2. In the **Timeout Duration** field, specify the timeout value, in seconds, for request retransmissions.

   Consideration to maximum delay time should be given when configuring RADIUS max retransmit and RADIUS timeout. If multiple RADIUS servers are configured, the max retransmit value on each will be exhausted before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the sum of (retransmit times timeout) for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.

3. From the **Accounting Mode** menu, select whether the RADIUS accounting mode is enabled or disabled on the current server.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

5. If you make changes to the page, click **Apply** to apply the changes to the system.

**RADIUS Server Configuration**

Use the RADIUS Server Configuration page to view and configure various settings for the current RADIUS server configured on the system.

To access the RADIUS Server **Configuration** page, click **Security > Management Security, and then click the RADIUS > Server Configuration** link.
To configure a RADIUS server:

1. To add a RADIUS server, specify the settings the following list describes, and click Add.
   - In the Server Address field, specify the IP address of the RADIUS server to add.
   - In the Authentication Port field, specify the UDP port number the server uses to verify the RADIUS server authentication. The valid range is 0–65535.
   - From the Secret Configured menu, select Yes to add a RADIUS secret in the next field. You must select Yes before you can configure the RADIUS secret. After you add the RADIUS server, this field indicates whether the shared secret for this server has been configured.
   - In the Secret field, type the shared secret text string used for authenticating and encrypting all RADIUS communications between the switch and the RADIUS server. This secret must match the RADIUS encryption.
   - From the Active menu, specify whether the server is a Primary or Secondary server.
   - From the Message Authenticator menu, enable or disable the message authenticator attribute for the selected server.

2. To modify settings for a RADIUS server that is already configured on the switch, select the check box next to the server address, update the desired fields, and click Apply.

3. Click Refresh to update the page with the most current information.

4. To delete a configured RADIUS server, select the check box next to the server address, and then click Delete.

5. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

The following table describes the RADIUS server statistics available on the page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
<td>This displays all configured RADIUS servers.</td>
</tr>
<tr>
<td>Round Trip Time</td>
<td>The time interval, in hundredths of a second, between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.</td>
</tr>
</tbody>
</table>
Use the buttons at the bottom of the page to perform the following actions:

- **Click Clear Counters** to clear the authentication server and RADIUS statistics to their default values.
- **Click Refresh** to refresh the page with the most current data from the switch.

**Accounting Server Configuration**

Use the RADIUS Accounting Server Configuration page to view and configure various settings for one or more RADIUS accounting servers on the network.

To access the RADIUS Accounting Server Configuration page, click **Security > Management Security > RADIUS > Accounting Server Configuration.**
To configure the RADIUS accounting server:

1. In the **Accounting Server Address** field, specify the IP address of the RADIUS accounting server to add.

2. In the **Port** field, specify the UDP port number the server uses to verify the RADIUS accounting server authentication. The valid range is 0–65535.

3. From the **Secret Configured** menu, select Yes to add a RADIUS secret in the next field. You must select Yes before you can configure the RADIUS secret. After you add the RADIUS accounting server, this field indicates whether the shared secret for this server has been configured.

4. In the **Secret** field, type the shared secret to use with the specified accounting server.

5. From the **Accounting Mode** menu, enable or disable the RADIUS accounting mode.

6. Click **Apply** to update the switch with the RADIUS Accounting server settings.

7. To delete a configured RADIUS Accounting server, click **Delete**.

8. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
The following table describes RADIUS accounting server statistics available on the page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Server Address</td>
<td>Displays the IP address of the supported RADIUS accounting server.</td>
</tr>
<tr>
<td>Round Trip Time (secs)</td>
<td>Displays the time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.</td>
</tr>
<tr>
<td>Accounting Requests</td>
<td>The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.</td>
</tr>
<tr>
<td>Accounting Retransmissions</td>
<td>The number of RADIUS Accounting-Request packets retransmitted to this server.</td>
</tr>
<tr>
<td>Accounting Responses</td>
<td>Displays the number of RADIUS packets received on the accounting port from this server.</td>
</tr>
<tr>
<td>Malformed Accounting Responses</td>
<td>Displays the number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.</td>
</tr>
<tr>
<td>Bad Authenticators</td>
<td>Displays the number of RADIUS Accounting-Response packets that contained invalid authenticators received from this accounting server.</td>
</tr>
<tr>
<td>Pending Requests</td>
<td>The number of RADIUS Accounting-Request packets destined for this server that have not yet timed out or received a response.</td>
</tr>
<tr>
<td>Timeouts</td>
<td>The number of accounting timeouts to this server.</td>
</tr>
<tr>
<td>Unknown Types</td>
<td>The number of RADIUS packets of unknown type which were received from this server on the accounting port.</td>
</tr>
<tr>
<td>Packets Dropped</td>
<td>The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.</td>
</tr>
</tbody>
</table>

Use the buttons at the bottom of the page to perform the following actions:

- Click **Clear Counters** to reset all statistics to their default value.
- Click **Refresh** to update the page with the most current information.
Configuring TACACS+

TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. TACACS+ provides the following services:

- **Authentication**: Provides authentication during login and via user names and user-defined passwords.
- **Authorization**: Performed at login. When the authentication session is completed, an authorization session starts using the authenticated user name. The TACACS+ server checks the user privileges.

The TACACS+ protocol ensures network security through encrypted protocol exchanges between the device and TACACS+ server.

The TACACS+ folder contains links to the following features:

- **Configuring TACACS+** on page 153
- **TACACS+ Server Configuration** on page 154

**TACACS+ Configuration**

The TACACS+ Configuration page contains the TACACS+ settings for communication between the switch and the TACACS+ server you configure via the inband management port.

To display the TACACS+ Configuration page, click **Security > Management Security, and then click the TACACS+ > TACACS+ Configuration link.**

To configure global TACACS+ settings:

1. In the **Key String** field, specify the authentication and encryption key for TACACS+ communications between the GS108T or GS110TP and the TACACS+ server. The valid range is 0–128 characters. The key must match the key configured on the TACACS+ server.

2. In the **Connection Timeout** field, specify the maximum number of seconds allowed to establish a TCP connection between the GS108T or GS110TP and the TACACS+ server. The valid range is 1–30 seconds.
3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

4. If you make any changes to the page, click **Apply** to apply the new settings to the system.

**TACACS+ Server Configuration**

Use the TACACS+ Server Configuration page to configure up to five TACACS+ servers with which the switch can communicate.

To display the TACACS+ Server Configuration page, click **Security** > **Management Security**, and then click the **TACACS+ > Server Configuration** link.

To configure TACACS+ server settings:

1. To add a new TACACS+ server, select **Add** from the **TACACS+ Server** field, enter the IP address of the server to add, and click **Apply**.

   **Note:** The **Add** option is available if fewer than five TACACS+ servers are configured on the system, and the **Server Address** field is only available when Add is selected in the TACACS+ Server IP Address field.

After you add one or more TACACS+ servers, additional fields appear on the TACACS+ Server Configuration page.
2. In the **Priority** field, specify the order in which the TACACS+ servers are used. A value of 0 is the highest priority.

3. In the **Port** field, specify the authentication port number through which the TACACS+ session occurs. The default is port 49, and the range is 0–65535.

4. In the **Key String** field, specify the authentication and encryption key for TACACS+ communications between the GS108T or GS110TP and the TACACS+ server. This key must match the encryption used on the TACACS+ server. The valid range is 0–128 characters.

5. In the **Connection Timeout** field, specify the amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is from 1 to 30 seconds.

6. If you make changes to the page, or add a new entry, click **Apply** to apply the changes to the system.

7. To delete a configured TACACS+ server, select the IP address of the server from the **TACACS+ Server** drop down menu, and then click **Delete**.

### Authentication List Configuration

Use the Authentication List page to configure the default login list. A login list specifies one or more authentication methods to validate switch or port access for the **admin** user.

**Note:** **Admin** is the only user on the system and is assigned to a preconfigured list named defaultList, which you cannot delete.

To access the Authentication List page, click **Security** > **Management Security**, and then click the **Authentication List** link.

To change the authentication method for the defaultList:

1. Select the check box next to the defaultList name.
2. Use the drop down menu in the 1 column to select the authentication method that should appear first in the selected authentication login list. If you select a method that does not time out as the first method, such as 'local', no other method will be tried, even if you have specified more than one method. This parameter will not appear when you first create a new login list. User authentication occurs in the order the methods are selected. Possible methods are as follows:

- **Local**: The user's locally stored ID and password will be used for authentication. Since the local method does not time out, if you select this option as the first method, no other method will be tried, even if you have specified more than one method.

- **RADIUS**: The user's ID and password will be authenticated using the RADIUS server. If you select RADIUS or TACACS+ as the first method and an error occurs during the authentication, the switch uses Method 2 to authenticate the user.

- **TACACS+**: The user's ID and password will be authenticated using the TACACS+ server. If you select RADIUS or TACACS+ as the first method and an error occurs during the authentication, the switch attempts user authentication Method 2.

- **None**: The authentication method is unspecified. This option is only available for Method 2 and Method 3.

3. Use the menu in the 2 column to select the authentication method, if any, that should appear second in the selected authentication login list. This is the method that will be used if the first method times out. If you select a method that does not time out as the second method, the third method will not be tried. This parameter will not appear when you first create a new login list.

4. Use the menu in the 3 column to select the authentication method, if any, that should appear third in the selected authentication login list. This parameter will not appear when you first create a new login list.

5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

6. If you make changes to the page, click **Apply** to apply the changes to the system.
Configuring Management Access

From the Access page, you can configure HTTP and Secure HTTP access to the GS108T or GS110TP management interface. You can also configure Access Control Profiles and Access Rules.

The **Security > Access** tab contains the following folders:

- **HTTP Configuration** on page 157
- **Secure HTTP Configuration** on page 158
- **Certificate Download** on page 159
- **Access Profile Configuration** on page 161
- **Access Rule Configuration** on page 162

**HTTP Configuration**

Use the HTTP Configuration page to configure the HTTP server settings on the system.

To access the HTTP Configuration page, click the **Security tab**, **then click Access**, and **then click the HTTP > HTTP Configuration link**.

![HTTP Configuration Page](image)

To configure the HTTP server settings:

1. Enable or disable the Web Java Mode. This applies to both secure and un-secure HTTP connections. The currently configured value is shown when the Web page is displayed. The default value is Enable.

2. In the **HTTP Session Soft Timeout** field, specify the number of minutes an HTTP session can be idle before a timeout occurs.

   After the session is inactive for the configured amount of time, the administrator is automatically logged out and must re-enter the password to access the management interface. A value of zero corresponds to an infinite timeout. The default value is 5 minutes. The currently configured value is shown when the Web page is displayed.
3. In the **HTTP Session Hard Timeout** field, specify the hard timeout for HTTP sessions. This timeout is unaffected by the activity level of the session. The value must be in the range of (0–168) hours. A value of zero corresponds to an infinite timeout. The default value is 24 hours. The currently configured value is shown when the Web page is displayed.

4. In the Maximum Number of HTTP Sessions field, specify the maximum number of HTTP sessions that can exist at the same time. The value must be in the range of (0–16). The default value is 16. The currently configured value is shown when the Web page is displayed.

5. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

6. If you make changes to the page, click **Apply** to apply the changes to the system.

**Secure HTTP Configuration**

Secure HTTP enables the transmission of HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. When you manage the switch by using a Web interface, secure HTTP can help ensure that communication between the management system and the switch is protected from eavesdroppers and man-in-the-middle attacks.

Use the Secure HTTP Configuration page to configure the settings for HTTPS communication between the management station and the switch.

To display the Secure HTTP Configuration page, click **Security > Access**, and then click the **HTTPS > HTTPS Configuration** link.

To configure HTTPS settings:

1. Use the radio buttons in the **HTTPS Admin Mode** field to enable or disable the Administrative Mode of Secure HTTP.
The currently configured value is shown when the Web page is displayed. The default value is Disable. You can only download SSL certificates when the HTTPS Admin mode is disabled.

2. Use the radio buttons in the SSL Version 3 field to enable or disable Secure Sockets Layer Version 3.0. The currently configured value is shown when the Web page is displayed. The default value is Enable.

3. Use the radio buttons in the TLS Version 1 field to enable or disable Transport Layer Security Version 1.0. The currently configured value is shown when the Web page is displayed. The default value is Enable.

4. In the HTTPS Port field, specify the TCP port to use for HTTPS data. The value must be in the range of 1–65535. Port 443 is the default value. The currently configured value is shown when the Web page is displayed.

5. In the HTTPS Session Soft Timeout field, specify the number of minutes an HTTPS session can be idle before a timeout occurs.

After the session is inactive for the configured amount of time, the administrator is automatically logged out and must re-enter the password to access the management interface. A value of zero corresponds to an infinite timeout. The default value is 5 minutes. The currently configured value is shown when the Web page is displayed.

6. In the HTTPS Session Hard Timeout field, specify the number of hours an HTTPS session can remain active, regardless of session activity. The value must be in the range of (1–168) hours. The default value is 24 hours. The currently configured value is shown when the Web page is displayed.

7. In the Maximum Number of HTTPS Sessions field, specify the maximum number of HTTPS sessions that can be open at the same time. The value must be in the range of (0–2). The default value is 2. The currently configured value is shown when the Web page is displayed.

8. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

9. If you make changes to the page, click Apply to apply the changes to the system.

Certificate Download

For the Web server on the switch to accept HTTPS connections from a management station, the Web server needs a public key certificate. You can generate a certificate externally (for example, off-line) and download it to the switch.

To display the Certificate Download page, click Security > Access, and then click the HTTPS > Certificate Download link.

Downloading SSL Certificates

Before you download a file to the switch, the following conditions must be true:

- The file to download from the TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch has a path to the TFTP server.
To configure the certificate download settings for HTTPS sessions:

1. From the **File Type** menu, select the type of SSL certificate to download, which can be one of the following:

2. In the **TFTP Server IP** field, specify the address of the TFTP server. The address can be an IP address in standard x.x.x.x format or a hostname. The hostname must start with a letter of the alphabet. Make sure that the software image or other file to be downloaded is available on the TFTP server.

3. In the **Remote File Name** field, specify the name of the file to download, including the path. You may enter up to 32 characters.

4. Select the **Start File Transfer** check box.

5. Click **Apply** to start the transfer. A status message displays during the transfer and upon successful completion of the transfer.

6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
Access Profile Configuration

Use the Access Profile Configuration page to configure settings that control management access to the switch. Access profile configuration requires three steps:

1. Use the Access Profile Configuration page to create an access profile. To add rules to the profile, the access profile must be deactivated, which is the default setting.
2. Use the Access Rule Configuration page to add one or more access rules to the profile.
3. Return to the Access Profile Configuration page to activate the profile.

To access the Access Profile Configuration page, click Security > Access, and then click the Access Control > Access Profile Configuration link.

To configure an Access Profile:

1. In the Access Profile Name field, specify the name of the access profile to be added. The maximum length is 32 characters.
2. To activate an access profile, select the Activate Profile check box. You cannot add rules to an active profile.
3. To deactivate an access profile, select the Deactivate Profile check box.
4. To remove an access profile, select the Remove Profile check box. The access profile should be deactivated before removing the access profile.
5. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
6. If you make changes to the page, click Apply to apply the changes to the system.
The Profile Summary table shows the rules that are configured for the profile, as the following table describes.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Type</td>
<td>Identifies the action the rule takes, which is either Permit or Deny.</td>
</tr>
<tr>
<td>Service Type</td>
<td>Displays the type of service to allow or prohibit from accessing the switch management interface:</td>
</tr>
<tr>
<td></td>
<td>• SNMP</td>
</tr>
<tr>
<td></td>
<td>• HTTP</td>
</tr>
<tr>
<td></td>
<td>• HTTPS</td>
</tr>
<tr>
<td>Source IP Address</td>
<td>Displays the IP Address of the client that may or may not originate management traffic.</td>
</tr>
<tr>
<td>Mask</td>
<td>Displays the subnet mask associated with the IP address.</td>
</tr>
<tr>
<td>Priority</td>
<td>Displays the priority of the rule. The rules are validated against the incoming management request in the ascending order of their priorities. If a rule matches, action is performed and subsequent rules below are ignored.</td>
</tr>
</tbody>
</table>

Click **Refresh** to update the page with the most current information.

**Access Rule Configuration**

Use the Access Rule Configuration page to configure the rules about what systems can access the GS108T or GS110TP Web interface and what protocols are allowed.

To access the Access Rule Configuration page, click **Security** > **Access**, and then click the **Access Control** > **Access Rule Configuration** link.
Before you create access rules, make sure:

- An access profile exists.
- The access profile is deactivated.

To configure access profile rules:

1. To add an access profile rule, configure the following settings and click **Add**.
   - **Rule Type**: Specify whether the rule permits or denies access to the GS108T or GS110TP management interface.
     - Select **Permit** to allow access to the management interface for traffic that meets the criteria you configure for the rule. Any traffic that does not meet the rules is denied.
     - Select **Deny** to prohibit access to the management interface for traffic that meets the criteria you configure for the rule. Any traffic that does not meet the rules is allowed access to the switch. Unlike MAC ACLs and IP ACLs, there is no implied *deny all* rule at the end of the rule list.
   - **Service Type**: Select the type of service to allow or prohibit from accessing the switch management interface:
     - SNMP
     - HTTP
     - HTTPS
   - **Source IP Address**: Specify the IP Address of the client originating the management traffic.
   - **Mask**: Specify the subnet mask associated with the IP address. The subnet mask is a standard subnet mask, and *not* an inverse (wildcard) mask that you use with IP ACLs.
   - **Priority**: Configure priority to the rule. The rules are validated against the incoming management request in the ascending order of their priorities. If a rule matches, action is performed and subsequent rules below are ignored. For example, if a Source IP 10.10.10.10 is configured with priority 1 to permit, and Source IP 10.10.10.10 is configured with priority 2 to Deny, then access is permitted if the profile is active, and the second rule is ignored.

2. To modify an access rule, select the check box next to the Rule Type, update the desired settings, and click **Apply**

3. To delete an access rule, select the check box next to the Rule Type, and click **Delete**.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
Port Authentication

In port-based authentication mode, when 802.1X is enabled globally and on the port, successful authentication of any one supplicant attached to the port results in all users being able to use the port without restrictions. At any given time, only one supplicant is allowed to attempt authentication on a port in this mode. Ports in this mode are under bidirectional control. This is the default authentication mode.

The 802.1X network has three components:

- **Authenticators:** Specifies the port that is authenticated before permitting system access.
- **Supplicants:** Specifies the host connected to the authenticated port requesting access to the system services.
- **Authentication Server:** Specifies the external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the user is authorized to access system services.

From the Port Authentication link, you can access the following pages:

- Basic:
  - 802.1X Configuration on page 164
- Advanced:
  - Port Authentication on page 165
  - Port Summary on page 169

802.1X Configuration

Use the 802.1X Configuration page to enable or disable port access control on the system.

To display the 802.1X Configuration page, click Security > Port Authentication > Basic > 802.1X Configuration.
To configure global 802.1X settings:

1. Select the appropriate radio button in the Port Based Authentication State field to enable or disable 802.1X administrative mode on the switch.
   - Enable. Port-based authentication is permitted on the switch.
   - Disable. The switch does not check for 802.1X authentication before allowing traffic on any ports, even if the ports are configured to allow only authenticated users.

2. Select the appropriate radio button in the Guest VLAN field to enable or disable the guest VLAN supplicant mode.
   - Enabled. When no 802.1X supplicant is authenticated on a port, the port still provides limited network access, as determined by a guest VLAN configured on the authentication server.
   - Disabled. A guest VLAN cannot be used for unauthorized ports.

3. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

4. If you change the settings, click Apply to apply the new settings to the system.

**Port Authentication**

Use the Port Authentication page to enable and configure port access control on one or more ports.

To access the Port Authentication page, click Security > Port Authentication, and then click the Advanced > Port Authentication link.

**Note:** Use the horizontal scroll bar at the bottom of the browser to view all the fields on the Port Authentication page. The following screen shots show the left and right halves of the Port Authentication page.
To configure 802.1X settings for the port:

1. Select the check box next to the port to configure. You can also select multiple check boxes to apply the same settings to the select ports, or select the check box in the heading row to apply the same settings to all ports.
2. For the selected port(s), specify the following settings:
   - **Port Control.** Defines the port authorization state. The control mode is only set if the link status of the port is link up. The possible field values are:
     - **Auto:** Automatically detects the mode of the interface.
     - **Authorized:** Places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication.
     - **Unauthorized:** Denies the selected interface system access by moving the interface into unauthorized state. The switch cannot provide authentication services to the client through the interface.
   - **Guest VLAN ID.** This field allows the user to configure the Guest VLAN ID on the interface. The valid range is 0–4093. The default value is 0. Enter 0 to reset the Guest VLAN ID on the interface.
   - **Guest VLAN Period.** This input field allows the user to enter the Guest VLAN period for the selected port. The Guest VLAN period is the value, in seconds, of the timer used by the Guest VLAN Authentication. The Guest VLAN timeout must be a value in the range of 1–300. The default value is 90.
   - **Periodic Reauthentication.** Use this field to enable or disable reauthentication of the supplicant for the specified port. Select Enable and Disable. If the value is Enable, reauthentication will occur. Otherwise, reauthentication will not be allowed. The default value is Disable. Changing the selection will not change the configuration until the Apply button is pressed.
   - **Reauthentication Period.** Indicates the time span in which the selected port is reauthenticated. The field value is in seconds. The range is 1–65535, and the field default is 3600 seconds.
   - **Quiet Period.** Defines the amount of time that the switch remains in the quiet state following a failed authentication exchange. The possible field range is 0–65535. The field value is in seconds. The field default is 60 seconds.
   - **Resending EAP.** This input field allows you to configure the transmit period for the selected port. The transmit period is the value, in seconds, of the timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identify frame to the supplicant. The transmit period must be a number in the range of 1–65535. The default value is 30. Changing the value will not change the configuration until you click the Apply button.
   - **Max EAP Requests.** This input field allows you to enter the maximum requests for the selected port. The maximum requests value is the maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The maximum requests value must be in the range of 1–10. The default value is 2. Changing the value will not change the configuration until you click the Apply button.
   - **Supplicant Timeout.** Defines the amount of time that lapses before EAP requests are resent to the user. The field value is in seconds. The field default is 30 seconds.
• **Server Timeout.** Defines the amount of time that lapses before the switch resends a request to the authentication server. The field value is in seconds. The range is 1–65535, and the field default is 30 seconds.

• **Control Direction.** This displays the control direction for the specified port, which is always Both. The control direction dictates the degree to which protocol exchanges take place between Supplicant and Authenticator. The unauthorized controlled port exerts control over communication in both directions (disabling both incoming and outgoing frames). This field is not configurable.

• **Protocol Version.** This field displays the protocol version associated with the selected port. The only possible value is 1, corresponding to the first version of the 802.1X specification. This field is not configurable.

• **PAE Capabilities.** This field displays the port access entity (PAE) functionality of the selected port. Possible values are Authenticator or Supplicant. This field is not configurable.

• **Authenticator PAE State.** This field displays the current state of the authenticator PAE state machine. Possible values are as follows:
  - Initialize
  - Disconnected
  - Connecting
  - Authenticating
  - Authenticated
  - Aborting
  - Held
  - ForceAuthorized
  - ForceUnauthorized

• **Backend State.** This field displays the current state of the backend authentication state machine. Possible values are as follows:
  - Request
  - Response
  - Success
  - Fail
  - Timeout
  - Initialize
  - Idle

• **EAPOL Flood Mode.** This field is used to enable or disable the EAPOL Flood mode per Interface. The default value is Disable.

3. Click **Apply** to send the updated screen to the switch and cause the changes to occur on the switch and the changes will be saved.
4. Click **Initialize** to begin the initialization sequence on the selected port(s). This button is only selectable if the control mode is *auto*. If the button is not selectable, it will be grayed out. When this button is clicked, the action is immediate. It is not required to click **Apply** for the action to occur.

5. Click **Reauthenticate** to begin the reauthentication sequence on the selected port. This button is only selectable if the control mode is *auto*. If the button is not selectable, it will be grayed out. When this button is pressed, the action is immediate. It is not required to click **Apply** for the action to occur.

6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

**Port Summary**

Use the Port Summary page to view information about the port access control settings on a specific port.

To access the Port Summary page, click **Security > Port Authentication > Advanced > Port Summary**.
The following table describes the fields on the Port Summary page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port whose settings are displayed in the current table row.</td>
</tr>
<tr>
<td>Control Mode</td>
<td>Defines the port authorization state. The control mode is only set if the</td>
</tr>
<tr>
<td></td>
<td>link status of the port is link up. The possible field values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>: Automatically detects the mode of the interface.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Force Authorized</strong>: Places the interface into an authorized state</td>
</tr>
<tr>
<td></td>
<td>without being authenticated. The interface sends and receives normal</td>
</tr>
<tr>
<td></td>
<td>traffic without client port-based authentication.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Force Unauthorized</strong>: Denies the selected interface system access by</td>
</tr>
<tr>
<td></td>
<td>moving the interface into unauthorized state. The switch cannot provide</td>
</tr>
<tr>
<td></td>
<td>authentication services to the client through the interface.</td>
</tr>
<tr>
<td>Operating Control Mode</td>
<td>This field indicates the control mode under which the port is actually</td>
</tr>
<tr>
<td></td>
<td>operating. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• ForceUnauthorized</td>
</tr>
<tr>
<td></td>
<td>• ForceAuthorized</td>
</tr>
<tr>
<td></td>
<td>• Auto</td>
</tr>
<tr>
<td></td>
<td>• N/A: If the port is in detached state it cannot participate in port access</td>
</tr>
<tr>
<td></td>
<td>control.</td>
</tr>
<tr>
<td>Reauthentication Enabled</td>
<td>Displays if reauthentication is enabled on the selected port. This is a</td>
</tr>
<tr>
<td></td>
<td>configurable field. The possible values are <strong>true</strong> and <strong>false</strong>. If the</td>
</tr>
<tr>
<td></td>
<td>value is <strong>true</strong>, reauthentication will occur. Otherwise, reauthentication</td>
</tr>
<tr>
<td></td>
<td>will not be allowed.</td>
</tr>
<tr>
<td>Port Status</td>
<td>This field displays the authorization status of the specified port. The</td>
</tr>
<tr>
<td></td>
<td>possible values are <strong>Authorized</strong>, <strong>Unauthorized</strong>, and <strong>N/A</strong>. If the</td>
</tr>
<tr>
<td></td>
<td>port is in detached state, the value will be <strong>N/A</strong> since the port cannot</td>
</tr>
<tr>
<td></td>
<td>participate in port access control.</td>
</tr>
</tbody>
</table>

Click **Refresh** to update the information on the screen.
Traffic Control

From the Traffic Control link, you can configure MAC Filters, Storm Control, Port Security, and Protected Port settings. To display the page, click the Security > Traffic Control tab.

The Traffic Control folder contains links to the following features:

- **MAC Filter**:
  - MAC Filter Configuration on page 171
  - MAC Filter Summary on page 173
- **Storm Control** on page 174
- **Port Security**:
  - Port Security Configuration on page 175
  - Port Security Interface Configuration on page 176
  - Security MAC Address on page 178
  - Protected Ports Membership on page 179

**MAC Filter Configuration**

Use the MAC Filter Configuration page to create MAC filters that limit the traffic allowed into and out of specified ports on the system.

To display the MAC Filter Configuration page, click Security > Traffic Control, and then click the MAC Filter > MAC Filter Configuration link.
To configure MAC filter settings:

1. To configure a new MAC filter:
   
a. Select Create Filter from the **MAC Filter** menu. If no filters have been configured, this is the only option available.

   b. From the VLAN ID menu, select the VLAN to use with the MAC address to fully identify packets you want filtered. You can change this field only when the Create Filter option is selected from the MAC Filter menu.

   c. In the MAC Address field, specify the MAC address of the filter in the format 00:01:1A:B2:53:4D. You can change this field when you have selected the Create Filter option.

      You cannot define filters for the following MAC addresses:
      
      • 00:00:00:00:00:00
      • 01:80:C2:00:00:00 to 01:80:C2:00:00:0F
      • 01:80:C2:00:00:20 to 01:80:C2:00:00:21
      • FF:FF:FF:FF:FF:FF

   d. Click the orange bar to display the available ports and select the port(s) to include in the inbound filter. If a packet with the MAC address and VLAN ID you specify is received on a port that is not in the list, it will be dropped.

   e. Click the orange bar to display the available ports and select the port(s) you to include in the outbound filter. Packets with the MAC address and VLAN ID you selected will be transmitted only out of ports that are in the list. Destination ports can be included only in the Multicast filter.

2. To delete a configured MAC Filter, select it from the menu, and then click **Delete**.

3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

4. If you make changes to the page, click **Apply** to apply the changes to the system.
MAC Filter Summary

Use the MAC Filter Summary page to view the MAC filters that are configured on the system. To display the MAC Filter Summary page, click Security > Traffic Control, and then click the MAC Filter > MAC Filter Summary link.

The following table describes the information displayed on the page:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Identifies the MAC address that is filtered.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID used with the MAC address to fully identify packets you want filtered. You can only change this field when you have selected the Create Filter option.</td>
</tr>
<tr>
<td>Source Port Members</td>
<td>Displays the ports included in the inbound filter.</td>
</tr>
<tr>
<td>Destination Port Members</td>
<td>Displays the ports included in the outbound filter.</td>
</tr>
</tbody>
</table>

Click Refresh to update the page with the most current information.
Storm Control

A broadcast storm is the result of an excessive number of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses can overload network resources and/or cause the network to time out.

The switch measures the incoming broadcast/multicast/unknown unicast packet rate per port and discards packets when the rate exceeds the defined value. Storm control is enabled per interface, by defining the packet type and the rate at which the packets are transmitted.

To display the Storm Control page, click Security > Traffic Control, and then click the Storm Control link.

To configure storm control settings:

1. Select the check box next to the port to configure. Select multiple check boxes to apply the same setting to all selected ports. Select the check box in the heading row to apply the same settings to all ports.

2. From the Ingress Control Mode menu, select the mode of broadcast affected by storm control.
   - Disable. Do not use storm control.
• **Unknown Unicast.** If the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped.

• **Multicast.** If the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped.

• **Broadcast.** If the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped.

3. In the **Threshold** field, specify the maximum rate at which unknown packets are forwarded. The range is a percent of the total threshold between 0–100%. The default is 5%.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

5. If you make changes to the page, click **Apply** to apply the changes to the system.

**Port Security Configuration**

Use the Port Security feature to lock one or more ports on the system. When a port is locked, only packets with an allowable source MAC addresses can be forwarded. All other packets are discarded.

To display the Port Security Configuration page, click **Security > Traffic Control, and then click the Port Security > Port Security Configuration link.**

To configure the global port security mode:

1. In the **Port Security Mode** field, select the appropriate radio button to enable or disable port security on the switch.

2. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

3. If you change the mode, click **Apply** to apply the change to the system.
The Port Security Violation table shows information about violations that occurred on ports that are enabled for port security. The following table describes the fields in the Port Security Violation table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Identifies the port where a violation occurred.</td>
</tr>
<tr>
<td>Last Violation MAC</td>
<td>Displays the source MAC address of the last packet that was discarded at a locked port.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Displays the VLAN ID corresponding to the Last Violation MAC address.</td>
</tr>
</tbody>
</table>

Click **Refresh** to refresh the page with the most current data from the switch.

**Port Security Interface Configuration**

A MAC address can be defined as allowable by one of two methods: dynamically or statically. Both methods are used concurrently when a port is locked.

Dynamic locking implements a first arrival mechanism for Port Security. You specify how many addresses can be learned on the locked port. If the limit has not been reached, then a packet with an unknown source MAC address is learned and forwarded normally. When the limit is reached, no more addresses are learned on the port. Any packets with source MAC addresses that were not already learned are discarded. You can effectively disable dynamic locking by setting the number of allowable dynamic entries to zero.

Static locking allows you to specify a list of MAC addresses that are allowed on a port. The behavior of packets is the same as for dynamic locking: only packets with an allowable source MAC address can be forwarded.

To display the Port Security Interface Configuration page, click **Security > Traffic Control, and then click the Port Security > Interface Configuration link.**
To configure port security settings:

1. To configure port security settings for a physical port, click PORTS.
2. To configure port security settings for a Link Aggregation Group (LAG), click LAGS.
3. To configure port security settings for both physical ports and LAGs, click ALL.
4. Select the check box next to the port or LAG to configure. Select multiple check boxes to apply the same setting to all selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.
5. Specify the following settings:
   - **Port Security.** Enable or Disable the port security feature for the selected port.
   - **Max Allowed Dynamically Learned MAC.** Sets the maximum number of dynamically learned MAC addresses on the selected interface. Valid range is 0–600.
   - **Max Allowed Statically Locked MAC.** Sets the maximum number of statically locked MAC addresses on the selected interface. Valid range is 0–20.
   - **Enable Violation Traps.** Enables or disables the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port.
6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
7. If you make changes to the page, click **Apply** to apply the changes to the system.
Security MAC Address

Use the Security MAC Address page to convert a dynamically learned MAC address to a statically locked address.

To display the Security MAC Address page, click Security > Traffic Control, and then click the Port Security > Security MAC Address link.

To convert learned MAC addresses:

1. Select the Convert Dynamic Address to Static check box.
2. Click Apply. The Dynamic MAC Address entries are converted to Static MAC address entries in a numerically ascending order until the Static limit is reached.

The Dynamic MAC Address Table shows the MAC addresses and their associated VLANs learned on the selected port. Use the Port List menu to select the interface for which you want to display data.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>Displays the VLAN ID corresponding to the Last Violation MAC address.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Displays the MAC addresses learned on a specific port.</td>
</tr>
</tbody>
</table>

Click Refresh to refresh the page with the most current data from the switch.
Protected Ports Membership

If a port is configured as protected, it does not forward traffic to any other protected port on the switch, but it will forward traffic to unprotected ports. Use the Protected Ports Membership page to configure the ports as protected or unprotected.

To display the Protected Ports Membership page, click the Security > Traffic Control > Protected Ports link.

To configure protected ports:

1. Click the orange bar to display the available ports.
2. Click the box below each port to configure as a protected port. Protected ports are marked with an X. No traffic forwarding is possible between two protected ports.
3. Click Refresh to refresh the page with the most current data from the switch.
4. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
5. If you make changes to the page, click Apply to apply the changes to the system. Configuration changes take effect immediately.
Configuring Access Control Lists

Access Control Lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and above all provide security for the network. The switch software supports IPv4 and MAC ACLs.

You first create an IPv4-based or MAC-based ACL ID. Then, you create a rule and assign it to a unique ACL ID. Next, you define the rules, which can identify protocols, source, and destination IP and MAC addresses, and other packet-matching criteria. Finally, use the ID number to assign the ACL to a port or to a LAG.

The Security > ACL folder contains links to the following features:

- **ACL Wizard** on page 180
- Basic:
  - **MAC ACL** on page 182
  - **MAC Rules** on page 183
  - **MAC Binding Configuration** on page 184
  - **MAC Binding Table** on page 186
- Advanced:
  - **IP ACL** on page 187
  - **IP Rules** on page 188
  - **IP Extended Rule** on page 189
  - **IP Binding Configuration** on page 193
  - **IP Binding Table** on page 194

**ACL Wizard**

The ACL Wizard simplifies the ACL rule configuration process. The Wizard contains a short list of access criteria that you can either permit or deny. When you select the permit or deny link associated with the access criteria, you are redirected to a page that is automatically configured with several of the settings.

**Note:** Before you use the ACL Wizard to configure rules, you must create either a MAC ACL, Standard IP ACL, or Extended IP ACL that will contain the rules. To create a MAC ACL, see **MAC ACL** on page 182. To create a standard or extended IP ACL, see **IP ACL** on page 187.

To display the ACL Wizard page, click Security > ACL.
To use the ACL Wizard:

1. Determine the type of ACL to configure and create a MAC ACL, standard IP ACL, or extended IP ACL.
   - To permit or deny traffic based on the Source MAC Address, create a MAC ACL.
   - To permit or deny traffic based on the Destination MAC Address, create a MAC ACL.
   - To permit or deny traffic based on the Source IP Address, create a Standard ACL.
   - To permit or deny traffic based on the Destination IP Address, create an Extended ACL.
   - To permit or deny traffic based on the TCP or UDP Source Port ID, create an Extended ACL.
   - To permit or deny traffic based on the TCP or UDP Destination Port ID, create an Extended ACL.

2. Click the Permit or Deny link associated with the access criteria on the ACL Wizard page.
   The switch redirects you to a page that contains the fields to configure the ACL rule, and several of the fields are preconfigured. For example, if you select the Permit link associated with the Select Devices Based on Source IP Address option, the Source IP Address Rules page displays, and the only information you must provide is the source IP address and source mask.

3. Configure the desired rule.

4. Click Apply to save the rule.
MAC ACL

A MAC ACL consists of a set of rules which are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken and the additional rules are not checked for a match.

There are multiple steps involved in defining a MAC ACL and applying it to the switch:

1. Use the MAC ACL page to create the ACL ID.
2. Use the MAC Rules page to create rules for the ACL.
3. Use the MAC Binding Configuration page to assign the ACL by its ID number to a port.
4. Optionally, use the MAC Binding Table page to view the configurations.

To display the MAC ACL page, click Security > ACL. The MAC ACL page is under the Basic link.

The MAC ACL table displays the number of ACLs currently configured in the switch and the maximum number of ACLs that can be configured. The current size is equal to the number of configured IPv4 ACLs plus the number of configured MAC ACLs.

To configure a MAC ACL:

1. To add a MAC ACL, specify a name for the MAC ACL in the Name field, and click Add. The name string may include alphabetic, numeric, dash, underscore, or space characters only. The name must start with an alphabetic character.

   Each configured ACL displays the following information:
   - **Rules**: Displays the number of rules currently configured for the MAC ACL.
   - **Direction**: Displays the direction of packet traffic affected by the MAC ACL, which can be Inbound or blank.

2. To delete a MAC ACL, select the check box next to the Name field, then click Delete.

3. To change the name of a MAC ACL, select the check box next to the Name field, update the name, then click Apply.
4. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

MAC Rules

Use the MAC Rules page to define rules for MAC-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. A default 'deny all' rule is the last rule of every list.

To display the MAC Rules page, click Security > ACL, then click the Basic > MAC Rules link.

To configure MAC ACL rules:

1. From the ACL Name field, specify the existing MAC ACL to which the rule will apply. To set up a new MAC ACL use the MAC ACL page.

2. To add a new rule, enter an ID for the rule, configure the following settings, and click Add.
   - **Action**. Specify what action should be taken if a packet matches the rule’s criteria:
     - **Permit**: Forwards packets that meet the ACL criteria.
     - **Deny**: Drops packets that meet the ACL criteria.
   - **Assign Queue**. Specifies the hardware egress queue identifier used to handle all packets matching this ACL rule. Enter an identifying number from 0–3 in this field.
   - **Match Every**. Requires a packet to match the criteria of this ACL. Select True or False from the drop down menu. Match Every is exclusive to the other filtering rules, so if Match Every is True, the other rules on the screen are not available.
   - **CoS**. Requires a packet’s class of service (CoS) to match the CoS value listed here. Enter a CoS value between 0–7 to apply this criteria.
   - **Destination MAC**. Requires an Ethernet frame’s destination port MAC address to match the address listed here. Enter a MAC address in this field. The valid format is xx:xx:xx:xx:xx:xx.
   - **Destination MAC Mask**. If desired, enter the MAC Mask associated with the Destination MAC to match. The MAC address mask specifies which bits in the destination MAC to compare against an Ethernet frame. Use Fs and zeros in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a zero in a bit position means that the data must equal the value given for that bit. For
example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is 00:00:ff:ff:ff:ff, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). A MAC mask of 00:00:00:00:00:00 matches a single MAC address.

- **EtherType Key.** Requires a packet’s EtherType to match the EtherType you select. Select the EtherType value from the drop down menu. If you select User Value, you can enter a custom EtherType value.

- **EtherType User Value.** This field is configurable if you select User Value from the EtherType drop down menu. The value you enter specifies a customized Ethertype to compare against an Ethernet frame. The valid range of values is 0x0600–0xFFFF.

- **Source MAC.** Requires a packet’s source port MAC address to match the address listed here. Enter a MAC address in the this field. The valid format is xx:xx:xx:xx:xx:xx.

- **Source MAC Mask.** If desired, enter the MAC mask for the source MAC address to match. Use Fs and zeros in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a zero in a bit position means that the data must equal the value given for that bit. The valid format is xx:xx:xx:xx:xx:xx. A MAC mask of 00:00:00:00:00:00 matches a single MAC address.

- **VLAN.** Requires a packet’s VLAN ID to match the ID listed here. Enter the VLAN ID to apply this criteria. The valid range is 1–4093.

3. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

4. To delete a rule, select the check box associated with the rule and click **Delete**.

5. To change a rule, select the check box associated with the rule, change the desired fields and click **Apply**.

### MAC Binding Configuration

When an ACL is bound to an interface, all the rules that have been defined are applied to the selected interface. Use the MAC Binding Configuration page to assign MAC ACL lists to ACL Priorities and Interfaces.

To display the MAC Binding Configuration page, click **Security > ACL, then click the Basic > MAC Binding Configuration** link.
To configure MAC ACL interface bindings:

1. Select an existing MAC ACL from the ACL ID menu.

   The packet filtering direction for ACL is Inbound, which means the MAC ACL rules are applied to traffic entering the port.

2. Specify an optional sequence number to indicate the order of this access list relative to other access lists already assigned to this interface and direction.

   A low number indicates high precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction will be used. The valid range is 1–4294967295.

3. Click the appropriate orange bar to expose the available ports or LAGs.
   - To add the selected ACL to a port or LAG, click the box directly below the port or LAG number so that an X appears in the box.
   - To remove the selected ACL from a port or LAG, click the box directly below the port or LAG number to clear the selection. An X in the box indicates that the ACL is applied to the interface.

4. Click Cancel to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

5. Click Apply to save any changes to the running configuration.
MAC Binding Table

Use the MAC Binding Table page to view or delete the MAC ACL bindings.

To display the MAC Binding Table, click **Security > ACL, then click the Basic > Binding Table** link.

The following table describes the information displayed in the **MAC Binding Table**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Displays the interface to which the MAC ACL is bound.</td>
</tr>
<tr>
<td>Direction</td>
<td>Specifies the packet filtering direction for ACL. The only valid direction</td>
</tr>
<tr>
<td></td>
<td>is Inbound, which means the MAC ACL rules are applied to traffic entering</td>
</tr>
<tr>
<td></td>
<td>the port.</td>
</tr>
<tr>
<td>ACL Type</td>
<td>Displays the type of ACL assigned to selected interface and direction.</td>
</tr>
<tr>
<td>ACL ID</td>
<td>Displays the ACL Name identifying the ACL assigned to selected interface and</td>
</tr>
<tr>
<td></td>
<td>direction.</td>
</tr>
<tr>
<td>Sequence N</td>
<td>Displays the Sequence Number signifying the order of specified ACL relative to other ACLs assigned to selected interface and direction.</td>
</tr>
</tbody>
</table>

To delete a MAC ACL-to-interface binding, select the check box next to the interface and click **Delete**.
IP ACL

IP ACLs allow network managers to define classification actions and rules for specific ingress ports. Packets can be filtered on ingress (inbound) ports only. If the filter rules match, then some actions can be taken, including dropping the packet or disabling the port. For example, a network administrator defines an ACL rule that says port number 20 can receive TCP packets. However, if a UDP packet is received the packet is dropped.

ACLs are composed of access control entries (ACE), or rules, that consist of the filters that determine traffic classifications.

Use the IP ACL Configuration page to add or remove IP-based ACLs.

To display the IP ACL page, click Security > ACL, then click the Advanced > IP ACL link.

The IP ACL area shows the current size of the ACL table versus the maximum size of the ACL table. The current size is equal to the number of configured IPv4 plus the number of configured MAC ACLs. The maximum size is 100.

To configure an IP ACL:

1. In the IP ACL ID field, specify the ACL ID. The ID is an integer in the following range:
   - 1–99: Creates an IP Standard ACL, which allows you to permit or deny traffic from a source IP address.
   - 100–199: Creates an IP Extended ACL, which allows you to permit or deny specific types of layer 3 or layer 4 traffic from a source IP address to a destination IP address. This type of ACL provides more granularity and filtering capabilities than the standard IP ACL.

Each configured ACL displays the following information:

- **Rules**: Displays the number of rules currently configured for the IP ACL.
- **Type**: Identifies the ACL as either a standard or extended IP ACL.
2. To delete an IP ACL, select the check box next to the IP ACL ID field, then click **Delete**.
3. To change the name of an IP ACL, select the check box next to the IP ACL ID field, update the name, then click **Apply**.
4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

**IP Rules**

Use the IP Rules page to define rules for IP-based standard ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

**Note:** There is an implicit “deny all” rule at the end of an ACL list. This means that if an ACL is applied to a packet and if none of the explicit rules match, then the final implicit “deny all” rule applies and the packet is dropped.

To display the IP Rules page, click **Security > ACL**, then click the **Advanced > IP Rules** link.

To configure rules for an IP ACL:

1. To add an IP ACL rule, select the ACL ID to add the rule to, complete the fields described in the following list, and click **Add**.
   - **Rule ID.** Specify a number from 1–10 to identify the IP ACL rule. You can create up to 10 rules for each ACL.
   - **Action.** Selects the ACL forwarding action, which is one of the following:
     - **Permit.** Forwards packets which meet the ACL criteria.
     - **Deny.** Drops packets which meet the ACL criteria.
• **Assign Queue ID.** Specifies the hardware egress queue identifier used to handle all packets matching this ACL rule. Enter an identifying number from 0–3 in the appropriate field.

• **Match Every.** Requires a packet to match the criteria of this ACL. Select True or False from the drop down menu. Match Every is exclusive to the other filtering rules, so if Match Every is True, the other rules on the screen are not available.

• **Source IP Address.** Requires a packet’s source IP address to match the address listed here. Type an IP Address in the appropriate field using dotted-decimal notation. The address you enter is compared to a packet’s source IP Address.

• **Source IP Mask.** Specifies the source IP address wildcard mask. Wild card masks determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all of the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. For example, to apply the rule to all hosts in the 192.168.1.0/24 subnet, you type 0.0.0.255 in the Source IP Mask field. This field is required when you configure a source IP address.

2. To delete an IP ACL rule, select the check box associated with the rule, and then click **Delete**.

3. To update an IP ACL rule, select the check box associated with the rule, update the desired fields, and then click **Apply**. You cannot modify the Rule ID of an existing IP rule.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

5. If you change any of the settings on the page, click **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

**IP Extended Rule**

Use the IP Extended Rules page to define rules for IP-based extended ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

---

**Note:** There is an implicit “deny all” rule at the end of an ACL list. This means that if an ACL is applied to a packet and if none of the explicit rules match, then the final implicit “deny all” rule applies and the packet is dropped.

---

To display the IP extended Rules page, click **Security > ACL, then click the Advanced > IP Extended Rules** link.
To configure rules for an IP ACL:

1. To add an IP ACL rule, select the ACL ID to add the rule to, select the check box in the Extended ACL Rule table, and click **Add**. The page displays the extended ACL Rule Configuration fields, as the following figure shows.

2. Configure the new rule.
   - **Rule ID**: Specify a number from 1–10 to identify the IP ACL rule. You can create up to 10 rules for each ACL.
• **Action.** Selects the ACL forwarding action, which is one of the following:
  • Permit. Forwards packets which meet the ACL criteria.
  • Deny. Drops packets which meet the ACL criteria.

• **Egress Queue.** Specifies the hardware egress queue identifier used to handle all packets matching this ACL rule. Enter an identifying number from 0–3 in the appropriate field.

• **Match Every.** Requires a packet to match the criteria of this ACL. Select True or False from the drop down menu. Match Every is exclusive to the other filtering rules, so if Match Every is True, the other rules on the screen are not available.

• **Protocol Type.** Requires a packet’s protocol to match the protocol listed here. Select a type from the drop down menu or enter the protocol number in the available field.

• **Src IP Address.** Requires a packet’s source IP address to match the address listed here. Type an IP Address in the appropriate field using dotted-decimal notation. The address you enter is compared to a packet's source IP Address.

• **Src IP Mask.** Specifies the source IP address wildcard mask. Wild card masks determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all of the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. For example, to apply the rule to all hosts in the 192.168.1.0/24 subnet, you type 0.0.0.255 in the Source IP Mask field. This field is required when you configure a source IP address.

• **Src L4 Port.** Requires a packet’s TCP/UDP source port to match the port listed here. Click Complete one of the following fields:
  • Source L4 Keyword: Select the desired L4 keyword from a list of source ports on which the rule can be based.
  • Source L4 Port Number: If the source L4 keyword is Other, enter a user-defined Port ID by which packets are matched to the rule.

• **Dst IP Address.** Requires a packet’s destination port IP address to match the address listed here. Enter an IP Address in the appropriate field using dotted-decimal notation. The address you enter is compared to a packet's destination IP Address.

• **Dst IP Mask.** Specifies the destination IP address wildcard mask. Wild card masks determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all of the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. For example, to apply the rule to all hosts in the 192.168.1.0/24 subnet, you type 0.0.0.255 in the Source IP Mask field. This field is required when you configure a source IP address.

• **Dst L4 Port.** Requires a packet’s TCP/UDP destination port to match the port listed here. Complete one of the following fields:
  • Destination L4 Keyword: Select the desired L4 keyword from a list of destination ports on which the rule can be based.
• Destination L4 Port Number: If the destination L4 keyword is Other, enter a user-defined Port ID by which packets are matched to the rule.

• **Service Type.** Choose one of the Service Type match conditions for the extended IP ACL rule. The possible values are IP DSCP, IP precedence, and IP TOS, which are alternative ways of specifying a match criterion for the same Service Type field in the IP header, however each uses a different user notation. After you select the service type, specify the value associated with the type.
  
  • IP DSCP: Specify the IP DiffServ Code Point (DSCP) value. The DSCP is defined as the high-order six bits of the Service Type octet in the IP header. Select an IP DSCP value from the menu. To specify a numeric value in the available field, select Other from the menu and type an integer from 0 to 63 in the field.
  
  • IP Precedence: The IP Precedence field in a packet is defined as the high-order three bits of the Service Type octet in the IP header. This is an optional configuration. Enter an integer from 0 to 7.
  
  • IP TOS Bits: Matches on the Type of Service bits in the IP header when checked. In the first TOS field, specify the two-digit hexadecimal TOS number. The second field is for the TOS Mask, which specifies the bit positions that are used for comparison against the IP TOS field in a packet. The TOS Mask value is a two-digit hexadecimal number from 00 to ff, representing an inverted (i.e. wildcard) mask. The zero-valued bits in the TOS Mask denote the bit positions in the TOS Bits value that are used for comparison against the IP TOS field of a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a TOS Bits value of a0 and a TOS Mask of 00.

3. To delete an IP ACL rule, select the check box associated with the rule, and then click **Delete.**

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

5. To modify an existing IP Extended ACL rule, click the Rule ID. The number is a hyperlink to the Extended ACL Rule Configuration page.
IP Binding Configuration

When an ACL is bound to an interface, all the rules that have been defined are applied to the selected interface. Use the IP Binding Configuration page to assign ACL lists to ACL Priorities and Interfaces.

To display the IP Binding Configuration page, click **Security > ACL**, then click the **Advanced > IP Binding Configuration** link.

To configure IP ACL interface bindings:

1. Select an existing IP ACL from the ACL ID menu.
   The packet filtering direction for ACL is Inbound, which means the IP ACL rules are applied to traffic entering the port.

2. Specify an optional sequence number to indicate the order of this access list relative to other access lists already assigned to this interface and direction.
   A low number indicates high precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction will be used. The valid range is 1–4294967295.

3. Click the appropriate orange bar to expose the available ports or LAGs.
   • To add the selected ACL to a port or LAG, click the box directly below the port or LAG number so that an X appears in the box.
   • To remove the selected ACL from a port or LAG, click the box directly below the port or LAG number to clear the selection. An X in the box indicates that the ACL is applied to the interface.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

5. Click **Apply** to save any changes to the running configuration.
IP Binding Table

Use the IP Binding Table page to view or delete the IP ACL bindings.

To display the IP Binding Table, click **Security** > **ACL**, then click the **Advanced** > **Binding Table** link.

The following table describes the information displayed in the **MAC Binding Table**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Displays the interface to which the IP ACL is bound.</td>
</tr>
<tr>
<td>Direction</td>
<td>Specifies the packet filtering direction for ACL. The only valid direction is Inbound, which means the IP ACL rules are applied to traffic entering the port.</td>
</tr>
<tr>
<td>ACL Type</td>
<td>Displays the type of ACL assigned to selected interface and direction.</td>
</tr>
<tr>
<td>ACL ID</td>
<td>Displays the ACL Number identifying the ACL assigned to selected interface and direction.</td>
</tr>
<tr>
<td>Seq No.</td>
<td>Displays the Sequence Number signifying the order of specified ACL relative to other ACLs assigned to selected interface and direction.</td>
</tr>
</tbody>
</table>

To delete an IP ACL-to-interface binding, select the check box next to the interface and click **Delete**.
Monitoring the System

Use the features available from the Monitoring tab to view a variety of information about the switch and its ports and to configure how the switch monitors events. The Monitoring tab contains links to the following features:

- **Ports** on page 196
- **System Logs** on page 208
- **Port Mirroring** on page 216
Ports

The pages available from the Ports link contain a variety of information about the number and type of traffic transmitted from and received on the switch. From the Ports link, you can access the following pages:

- **Switch Statistics** on page 196
- **Port Statistics** on page 198
- **Port Detailed Statistics** on page 199
- **EAP Statistics** on page 206

Switch Statistics

The Switch Statistics page displays detailed statistical information about the traffic the switch handles.

To access the Switch Statistics page, click **Monitoring > Ports > Switch Statistics**.
The following table describes the Switch Statistics displayed on the screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifIndex</td>
<td>This object indicates the ifIndex of the interface table entry associated with the processor of this switch.</td>
</tr>
<tr>
<td>Octets Received</td>
<td>The total number of octets of data received by the processor (excluding framing bits, but including FCS octets).</td>
</tr>
<tr>
<td>Packets Received Without Errors</td>
<td>The total number of packets (including broadcast packets and multicast packets) received by the processor.</td>
</tr>
<tr>
<td>Unicast Packets Received</td>
<td>The number of subnetwork-unicast packets delivered to a higher layer protocol.</td>
</tr>
<tr>
<td>Multicast Packets Received</td>
<td>The total number of packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.</td>
</tr>
<tr>
<td>Broadcast Packets Received</td>
<td>The total number of packets received that were directed to the broadcast address. This does not include multicast packets.</td>
</tr>
<tr>
<td>Receive Packets Discarded</td>
<td>The number of inbound packets which were chosen to be discarded, even though no errors had been detected, in order to prevent their being delivered to a higher layer protocol. A possible reason for discarding a packet could be to free up buffer space.</td>
</tr>
<tr>
<td>Octets Transmitted</td>
<td>The total number of octets transmitted out of the interface, including framing characters.</td>
</tr>
<tr>
<td>Packets Transmitted Without Errors</td>
<td>The total number of packets transmitted out of the interface.</td>
</tr>
<tr>
<td>Unicast Packets Transmitted</td>
<td>The total number of packets that higher level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.</td>
</tr>
<tr>
<td>Multicast Packets Transmitted</td>
<td>The total number of packets that higher level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.</td>
</tr>
<tr>
<td>Broadcast Packets Transmitted</td>
<td>The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.</td>
</tr>
<tr>
<td>Transmit Packets Discarded</td>
<td>The number of outbound packets which were chosen to be discarded, even though no errors had been detected, in order to prevent their being delivered to a higher layer protocol. A possible reason for discarding a packet could be to free up buffer space.</td>
</tr>
<tr>
<td>Most Address Entries Ever Used</td>
<td>The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.</td>
</tr>
<tr>
<td>Address Entries in Use</td>
<td>The number of Learned and static entries in the Forwarding Database Address Table for this switch.</td>
</tr>
<tr>
<td>Maximum VLAN Entries</td>
<td>The maximum number of Virtual LANs (VLANs) allowed on this switch.</td>
</tr>
</tbody>
</table>
Click **Clear** to clear all the statistics counters, resetting all switch summary and detailed statistics to default values. The discarded packets count cannot be cleared.

Click **Refresh** to refresh the page with the most current data from the switch.

**Port Statistics**

The Port Statistics page displays a summary of per-port traffic statistics on the switch.

To access the Port Summary page, click **Monitoring** > **Ports**, and then click the Port Statistics link.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most VLAN Entries Ever Used</td>
<td>The largest number of VLANs that have been active on this switch since the last reboot.</td>
</tr>
<tr>
<td>Static VLAN Entries</td>
<td>The number of presently active VLAN entries on this switch that have been created statically.</td>
</tr>
<tr>
<td>Dynamic VLAN Entries</td>
<td>The number of presently active VLAN entries on this switch.</td>
</tr>
<tr>
<td>VLAN Deletes</td>
<td>The number of VLANs on this switch that have been created and then deleted since the last reboot.</td>
</tr>
<tr>
<td>Time Since Counters Last Cleared</td>
<td>The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.</td>
</tr>
</tbody>
</table>
The following table describes the per-port statistics displayed on the screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Lists the ports on the system.</td>
</tr>
<tr>
<td>Total Packets Received Without Errors</td>
<td>The total number of packets received that were without errors.</td>
</tr>
<tr>
<td>Packets Received With Error</td>
<td>The number of inbound packets that contained errors preventing them from being deliverable to a higher layer protocol.</td>
</tr>
<tr>
<td>Broadcast Packets Received</td>
<td>The total number of good packets received that were directed to the broadcast address. This does not include multicast packets.</td>
</tr>
<tr>
<td>Packets Transmitted Without Errors</td>
<td>The number of frames that have been transmitted by this port to its segment.</td>
</tr>
<tr>
<td>Transmit Packet Errors</td>
<td>The number of outbound packets that could not be transmitted because of errors.</td>
</tr>
<tr>
<td>Collision Frames</td>
<td>The best estimate of the total number of collisions on this Ethernet segment.</td>
</tr>
<tr>
<td>Time Since Counters Last Cleared</td>
<td>The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.</td>
</tr>
</tbody>
</table>

Use the buttons at the bottom of the page to perform the following actions:

- To clear all the counters for all ports on the switch, select the check box in the row heading and click **Clear**. The button resets all statistics for all ports to default values.
- To clear the counters for a specific port, select the check box associated with the port and click **Clear**.
- Click **Refresh** to refresh the data on the screen and display the most current statistics.

**Port Detailed Statistics**

The Port Detailed Statistics page displays a variety of per-port traffic statistics.

To access the Port Detailed page, click the **Monitoring > Ports tab, and then click Port Detailed Statistics**. (The following figure shows some, but not all, of the fields on the Port Detailed Statistics page.)
The following table describes the detailed port information displayed on the screen. To view information about a different port, select the port number from the Interface menu.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Use the drop down menu to select the interface for which data is to be displayed or configured.</td>
</tr>
<tr>
<td>MST ID</td>
<td>Displays the created or existing MSTs.</td>
</tr>
<tr>
<td>ifIndex</td>
<td>This field indicates the ifIndex of the interface table entry associated with this port on an adapter.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port Type</td>
<td>For most ports this field is blank. Otherwise the possible values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mirrored</strong>: Indicates that the port has been configured as a monitoring port and is the source port in a port mirroring session. For additional information about port monitoring and probe ports, see <em>Multiple Port Mirroring</em> on page 216.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Probe</strong>: Indicates that the port has been configured as a monitoring port and is the destination port in a port mirroring session. For additional information about port monitoring and probe ports, see <em>Multiple Port Mirroring</em> on page 216.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Port Channel</strong>: Indicates that the port has been configured as a member of a port-channel, which is also known as a link Aggregation Group (LAG).</td>
</tr>
<tr>
<td>Port Channel ID</td>
<td>If the port is a member of a port channel, the port channel's interface ID and name are shown. Otherwise, Disable is shown.</td>
</tr>
<tr>
<td>Port Role</td>
<td>Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.</td>
</tr>
<tr>
<td>STP Mode</td>
<td>Displays the Spanning Tree Protocol (STP) Administrative Mode for the port or LAG. The possible values for this field are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable</strong>: Enables the Spanning Tree Protocol for this port.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disable</strong>: Disables the Spanning Tree Protocol for this port.</td>
</tr>
<tr>
<td>STP State</td>
<td>Displays the port's current state Spanning Tree state. This state controls what action a port takes on receipt of a frame. If the bridge detects a malfunctioning port it will place that port into the broken state. The other five states are defined in IEEE 802.1D:</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
</tr>
<tr>
<td></td>
<td>• Blocking</td>
</tr>
<tr>
<td></td>
<td>• Listening</td>
</tr>
<tr>
<td></td>
<td>• Learning</td>
</tr>
<tr>
<td></td>
<td>• Forwarding</td>
</tr>
<tr>
<td></td>
<td>• Broken</td>
</tr>
<tr>
<td>Admin Mode</td>
<td>Displays the port control administration state:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable</strong>: The port can participate in the network (default).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disable</strong>: The port is administratively down and does not participate in the network.</td>
</tr>
<tr>
<td>LACP Mode</td>
<td>Selects the Link Aggregation Control Protocol administration state:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable</strong>: Specifies that the port is allowed to participate in a port channel (LAG), which is the default mode.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disable</strong>: Specifies that the port cannot participate in a port channel (LAG).</td>
</tr>
<tr>
<td>Physical Mode</td>
<td>Indicates the port speed and duplex mode. In auto-negotiation mode, the duplex mode and speed are set from the auto-negotiation process.</td>
</tr>
<tr>
<td>Physical Status</td>
<td>Indicates the port speed and duplex mode status.</td>
</tr>
<tr>
<td>Link Status</td>
<td>Indicates whether the link is up or down.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Link Trap</td>
<td>This object determines whether or not to send a trap when link status changes. The factory default is Enable.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable</strong>: Specifies that the system sends a trap when the link status changes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disable</strong>: Specifies that the system does not send a trap when the link status changes.</td>
</tr>
<tr>
<td>Packets RX and TX 64 Octets</td>
<td>The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets RX and TX 65-127 Octets</td>
<td>The total number of packets (including bad packets) received or transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets RX and TX 128-255 Octets</td>
<td>The total number of packets (including bad packets) received or transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets RX and TX 256-511 Octets</td>
<td>The total number of packets (including bad packets) received or transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets RX and TX 512-1023 Octets</td>
<td>The total number of packets (including bad packets) received or transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets RX and TX 1024-1518 Octets</td>
<td>The total number of packets (including bad packets) received or transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets RX and TX &gt; 1522 Octets</td>
<td>The total number of packets (including bad packets) received or transmitted that are in excess of 1522 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Octets Received</td>
<td>The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.</td>
</tr>
<tr>
<td>Packets Received 64 Octets</td>
<td>The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets Received 65-127 Octets</td>
<td>The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets Received 128-255 Octets</td>
<td>The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets Received 256-511 Octets</td>
<td>The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Packets Received 512-1023 Octets</td>
<td>The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets Received 1024-1518 Octets</td>
<td>The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets Received &gt; 1522 Octets</td>
<td>The total number of packets received that were in excess of 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.</td>
</tr>
<tr>
<td>Total Packets Received Without Errors</td>
<td>The total number of packets received that were without errors.</td>
</tr>
<tr>
<td>Unicast Packets Received</td>
<td>The number of subnetwork-unicast packets delivered to a higher-layer protocol.</td>
</tr>
<tr>
<td>Multicast Packets Received</td>
<td>The total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.</td>
</tr>
<tr>
<td>Broadcast Packets Received</td>
<td>The total number of good packets received that were directed to the broadcast address. This does not include multicast packets.</td>
</tr>
<tr>
<td>Total Packets Received with MAC Errors</td>
<td>The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.</td>
</tr>
<tr>
<td>Jabbers Received</td>
<td>The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). This definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.</td>
</tr>
<tr>
<td>Fragments Received</td>
<td>The total number of packets received that were less than 64 octets in length with ERROR CRC (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Undersize Received</td>
<td>The total number of packets received that were less than 64 octets in length with GOOD CRC (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Alignment Errors</td>
<td>The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.</td>
</tr>
<tr>
<td>Rx FCS Errors</td>
<td>The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets.</td>
</tr>
<tr>
<td>Overruns</td>
<td>The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.</td>
</tr>
<tr>
<td>Total Received Packets Not Forwarded</td>
<td>A count of valid frames received which were discarded (i.e., filtered) by the forwarding process.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Local Traffic Frames</td>
<td>The total number of frames dropped in the forwarding process because the destination address was located off of this port.</td>
</tr>
<tr>
<td>802.3x Pause Frames Received</td>
<td>A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.</td>
</tr>
<tr>
<td>Unacceptable Frame Type</td>
<td>The number of frames discarded from this port due to being an unacceptable frame type.</td>
</tr>
<tr>
<td>Multicast Tree Viable Discards</td>
<td>The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.</td>
</tr>
<tr>
<td>Reserved Address Discards</td>
<td>The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.</td>
</tr>
<tr>
<td>Broadcast Storm Recovery</td>
<td>The number of frames discarded that are destined for FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled.</td>
</tr>
<tr>
<td>CFI Discards</td>
<td>The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.</td>
</tr>
<tr>
<td>Upstream Threshold</td>
<td>The number of frames discarded due to lack of cell descriptors available for that packet's priority level.</td>
</tr>
<tr>
<td>Total Packets Transmitted (Octets)</td>
<td>The total number of octets of data (including those in bad packets) transmitted on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.</td>
</tr>
<tr>
<td>Packets Transmitted 64 Octets</td>
<td>The total number of packets (including bad packets) transmitted that were 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets Transmitted 65-127 Octets</td>
<td>The total number of packets (including bad packets) transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets Transmitted 128-255 Octets</td>
<td>The total number of packets (including bad packets) transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets Transmitted 256-511 Octets</td>
<td>The total number of packets (including bad packets) transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets Transmitted 512-1023 Octets</td>
<td>The total number of packets (including bad packets) transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets Transmitted 1024-1518 Octets</td>
<td>The total number of packets (including bad packets) transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Transmitted 1519-1522 Octets</td>
<td>The total number of packets (including bad packets) transmitted that were</td>
</tr>
<tr>
<td></td>
<td>between 1519 and 1522 octets in length inclusive (excluding framing bits but</td>
</tr>
<tr>
<td></td>
<td>including FCS octets).</td>
</tr>
<tr>
<td>Total Packets Transmitted Successfully</td>
<td>The number of frames that have been transmitted by this port to its segment.</td>
</tr>
<tr>
<td>Unicast Packets Transmitted</td>
<td>The total number of packets that higher-level protocols requested be</td>
</tr>
<tr>
<td></td>
<td>transmitted to a subnetwork-unicast address, including those that were</td>
</tr>
<tr>
<td></td>
<td>discarded or not sent.</td>
</tr>
<tr>
<td>Multicast Packets Transmitted</td>
<td>The total number of packets that higher-level protocols requested be</td>
</tr>
<tr>
<td></td>
<td>transmitted to a Multicast address, including those that were discarded or</td>
</tr>
<tr>
<td></td>
<td>not sent.</td>
</tr>
<tr>
<td>Broadcast Packets Transmitted</td>
<td>The total number of packets that higher-level protocols requested be</td>
</tr>
<tr>
<td></td>
<td>transmitted to the Broadcast address, including those that were discarded or</td>
</tr>
<tr>
<td></td>
<td>not sent.</td>
</tr>
<tr>
<td>Total Transmit Errors</td>
<td>The sum of Single, Multiple, and Excessive Collisions.</td>
</tr>
<tr>
<td>Tx FCS Errors</td>
<td>The total number of packets transmitted that had a length (excluding framing</td>
</tr>
<tr>
<td></td>
<td>bits, but including FCS octets) of between 64 and 1518 octets, inclusive,</td>
</tr>
<tr>
<td></td>
<td>but had a bad Frame Check Sequence (FCS) with an integral number of octets</td>
</tr>
<tr>
<td>Tx Oversized</td>
<td>The total number of frames that exceeded the max permitted frame size. This</td>
</tr>
<tr>
<td></td>
<td>counter has a max increment rate of 815 counts per second at 10 Mb/s.</td>
</tr>
<tr>
<td>Underrun Errors</td>
<td>The total number of frames discarded because the transmit FIFO buffer</td>
</tr>
<tr>
<td></td>
<td>became empty during frame transmission.</td>
</tr>
<tr>
<td>Total Transmit Packets Discarded</td>
<td>The sum of single collision frames discarded, multiple collision frames</td>
</tr>
<tr>
<td></td>
<td>discarded, and excessive frames discarded.</td>
</tr>
<tr>
<td>Single Collision Frames</td>
<td>A count of the number of successfully transmitted frames on a particular</td>
</tr>
<tr>
<td></td>
<td>interface for which transmission is inhibited by exactly one collision.</td>
</tr>
<tr>
<td>Multiple Collision Frames</td>
<td>A count of the number of successfully transmitted frames on a particular</td>
</tr>
<tr>
<td></td>
<td>interface for which transmission is inhibited by more than one collision.</td>
</tr>
<tr>
<td>Excessive Collision Frames</td>
<td>A count of frames for which transmission on a particular interface fails due</td>
</tr>
<tr>
<td></td>
<td>to excessive collisions.</td>
</tr>
<tr>
<td>Port Membership Discards</td>
<td>The number of frames discarded on egress for this port due to egress filtering</td>
</tr>
<tr>
<td></td>
<td>being enabled.</td>
</tr>
<tr>
<td>STP BPDUs Received</td>
<td>Number of STP BPDUs received at the selected port.</td>
</tr>
<tr>
<td>STP BPDUs Transmitted</td>
<td>Number of STP BPDUs transmitted from the selected port.</td>
</tr>
<tr>
<td>RSTP BPDUs Received</td>
<td>Number of RSTP BPDUs received at the selected port.</td>
</tr>
<tr>
<td>RSTP BPDUs Transmitted</td>
<td>Number of RSTP BPDUs transmitted from the selected port.</td>
</tr>
<tr>
<td>MSTP BPDUs Received</td>
<td>Number of MSTP BPDUs received at the selected port.</td>
</tr>
<tr>
<td>MSTP BPDUs Transmitted</td>
<td>Number of MSTP BPDUs transmitted from the selected port.</td>
</tr>
</tbody>
</table>
Use the buttons at the bottom of the page to perform the following actions:

- Click **Clear** to clear all the counters. This resets all statistics for this port to the default values.
- Click **Refresh** to refresh the data on the screen and display the most current statistics.

**EAP Statistics**

Use the EAP Statistics page to display information about EAP packets received on a specific port.

To display the EAP Statistics page, click the **Monitoring > Ports** tab, and then click the **EAP Statistics** link.
The following table describes the EAP statistics displayed on the screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td>Specifies the interface which is polled for statistics.</td>
</tr>
<tr>
<td>Frames Received</td>
<td>Displays the number of valid EAPOL frames received on the port.</td>
</tr>
<tr>
<td>Frames Transmitted</td>
<td>Displays the number of EAPOL frames transmitted through the port.</td>
</tr>
<tr>
<td>Start Frames Received</td>
<td>Displays the number of EAPOL Start frames received on the port.</td>
</tr>
<tr>
<td>Log off Frames Received</td>
<td>Displays the number of EAPOL Log off frames that have been received on the port.</td>
</tr>
<tr>
<td>Last Frame Version</td>
<td>Displays the protocol version number attached to the most recently received EAPOL frame.</td>
</tr>
<tr>
<td>Last Frame Source</td>
<td>Displays the source MAC Address attached to the most recently received EAPOL frame.</td>
</tr>
<tr>
<td>Invalid Frames Received</td>
<td>Displays the number of unrecognized EAPOL frames received on this port.</td>
</tr>
<tr>
<td>Length Error Frames Received</td>
<td>Displays the number of EAPOL frames with an invalid Packet Body Length received on this port.</td>
</tr>
<tr>
<td>Response/ID Frames Received</td>
<td>Displays the number of EAP Respond ID frames that have been received on the port.</td>
</tr>
<tr>
<td>Response Frames Received</td>
<td>Displays the number of valid EAP Response frames received on the port.</td>
</tr>
<tr>
<td>Request/ID Frames Transmitted</td>
<td>Displays the number of EAP Requested ID frames transmitted through the port.</td>
</tr>
<tr>
<td>Request Frames Transmitted</td>
<td>Displays the number of EAP Request frames transmitted through the port.</td>
</tr>
</tbody>
</table>

Use the buttons at the bottom of the page to perform the following actions:

- To clear all the EAP counters for all ports on the switch, select the check box in the row heading and click **Clear**. The button resets all statistics for all ports to default values.
- To clear the counters for a specific port, select the check box associated with the port and click **Clear**.
- Click **Refresh** to refresh the data on the screen and display the most current statistics.
System Logs

The switch may generate messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences. These messages are stored locally and can be forwarded to one or more centralized points of collection for monitoring purposes or long term archival storage. Local and remote configuration of the logging capability includes filtering of messages logged or forwarded based on severity and generating component.

The Monitoring > Logs tab contains links to the following folders:

- Memory Logs on page 208
- FLASH Log Configuration on page 210
- Server Log Configuration on page 212
- Trap Logs on page 214
- Event Logs on page 215

Memory Logs

The in-memory log stores messages in memory based upon the settings for message component and severity. Use the Memory Logs page to set the administrative status and behavior of logs in the system buffer. These log messages are cleared when the switch reboots.

To access the Memory Log page, click the Monitoring > Logs tab, and then click the Memory Log link.
To configure the Memory Log settings:

1. Use the radio buttons in the **Admin Status** field to determine whether to log messages.
   - **Enable**: Enables system logging.
   - **Disable**: Prevents the system from logging messages.

2. From the **Behavior** menu, specify the behavior of the log when it is full.
   - **Wrap**: When the buffer is full, the oldest log messages are deleted as the system logs new messages.
   - **Stop on Full**: When the buffer is full, the system stops logging new messages and preserves all existing log messages.

3. If you change the buffered log settings, click **Apply** to apply the changes to the system and the changes will be saved.

The Memory Log table also appears on the Memory Log page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Number of Messages</td>
<td>Displays the number of messages the system has logged in memory. Only the 64 most recent entries are displayed on the page.</td>
</tr>
</tbody>
</table>

The rest of the page displays the Memory Log messages. The format of the log message is the same for messages that are displayed for the message log, persistent log, or console log. Messages logged to a collector or relay via syslog have the same format as well.

The following example shows the standard format for a log message:

```
<14> Mar 24 05:34:05 10.131.12.183-1 UNKN[2176789276]: main_login.c(179) 3855 %% HTTP Session 19 initiated for user admin connected from 10.27.64.122
```

The number contained in the angle brackets represents the message priority, which is derived from the following values:

Priority = (facility value × 8) + severity level.

The facility value is usually one, which means it is a user-level message. Therefore, to determine the severity level of the message, subtract eight from the number in the angle brackets. The example log message has a severity level of 6 (informational). For more information about the severity of a log message, see the **Severity Filter** description on page 213.

The message was generated on March 24 at 5:34:05 a.m by the switch with an IP address of 10.131.12.183. The component that generated the message is unknown, but it came from line 179 of the main_login.c file. This is the 3,855th message logged since the switch was last booted. The message indicates that the administrator logged onto the HTTP management interface from a host with an IP address of 10.27.64.122.
Use the buttons at the bottom of the page to perform the following actions:

- Click **Clear** to clear the messages out of the buffered log in the memory.
- Click **Refresh** to update the page with the latest messages in the log.
- Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

**FLASH Log Configuration**

The FLASH log is a log that is stored in persistent storage, which means that the log messages are retained across a switch reboot.

- The first log type is the **system startup log**. The system startup log stores the first N messages received after system reboot. This log always has the log full operation attribute set to stop on full and can store up to 32 messages.
- The second log type is the **system operation log**. The system operation log stores the last N messages received during system operation. This log always has the log full operation attribute set to overwrite. This log can store up to 1000 messages.

Either the system startup log or the system operation log stores a message received by the log subsystem that meets the storage criteria, but not both. On system startup, if the startup log is configured, it stores messages up to its limit. The operation log, if configured, then begins to store the messages.

Use the FLASH Log Configuration page to enable or disable persistent logging and to set the severity filter.

To access the FLASH Log Configuration page, click the **Monitoring > Logs** tab, and then click the **FLASH Log** link.
To configure the FLASH Log settings:

1. Use the radio buttons in the **Admin Status** field to determine whether to log messages to persistent storage.
   - **Enable**: Enables persistent logging.
   - **Disable**: Prevents the system from logging messages in persistent storage.

2. From the **Severity Filter** field, specify the type of log messages to record. A log records messages equal to or above a configured severity threshold. For example, if you select Error, the logged messages include Error, Critical, Alert, and Emergency. The default severity level is Alert(1). The severity can be one of the following levels:
   - **Emergency** (0): The highest level warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
   - **Alert** (1): The second highest warning level. An alert log is saved if there is a serious device malfunction, such as all device features being down. Action must be taken immediately.
   - **Critical** (2): The third highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
   - **Error** (3): A device error has occurred, such as if a port is offline.
   - **Warning** (4): The lowest level of a device warning.
   - **Notice** (5): Normal but significant conditions. Provides the network administrators with device information.
   - **Info** (6): Provides device information.
   - **Debug** (7): Provides detailed information about the log. Debugging should only be entered by qualified support personnel.

3. If you make any changes to the page, click **Apply** to apply the change to the system.

The rest of the page displays the number of persistent messages the system has logged and the persistent log messages.

Use the buttons at the bottom of the page to perform the following actions:

- Click **Clear** to clear the messages out of the buffered log.
- Click **Refresh** to refresh the page with the most current data from the switch.
- Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
Server Log Configuration

Use the Server Log Configuration page to allow the switch to send log messages to the remote logging hosts configured on the system.

To access the Server Log Configuration page, click the Monitoring > Logs tab, and then click the Server Log link.

To configure local log server settings:

1. Use the radio buttons in the Admin Status field to determine whether to send log messages to the remote syslog hosts configured on the switch.
   - Enable: Messages will be sent to all configured hosts (syslog collectors or relays) using the values configured for each host.
   - Disable: Stops logging to all syslog hosts. Disable means no messages will be sent to any collector/relay.

2. In the Local UDP Port field, specify the port on the switch from which syslog messages are sent.

3. Click Apply to save the settings.

The Server Log Configuration area also displays the following information:

- The Messages Relayed field shows the number of messages forwarded by the syslog function to a syslog host. **Messages forwarded to multiple hosts are counted once for each host.**
- The Messages Ignored field shows the number of messages that were ignored.
To configure a remote log server

1. To add a remote syslog host (log server), specify the settings in the following list and click **Add**.
   - **Host Address**: Specify the IP address or hostname of the host configured for syslog.
   - **Port**: Specify the port on the host to which syslog messages are sent. The default port is 514.
   - **Severity Filter**: Use the menu to select the severity of the logs to send to the logging host. Logs with the selected severity level and all logs of greater severity are sent to the host. For example, if you select Error, the logged messages include Error, Critical, Alert, and Emergency. The default severity level is Alert(1). The severity can be one of the following levels:
     - **Emergency (0)**: The highest level warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
     - **Alert (1)**: The second highest warning level. An alert log is saved if there is a serious device malfunction, such as all device features being down.
     - **Critical (2)**: The third highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
     - **Error (3)**: A device error has occurred, such as if a port is offline.
     - **Warning (4)**: The lowest level of a device warning.
     - **Notice (5)**: Provides the network administrators with device information.
     - **Informational (6)**: Provides device information.
     - **Debug (7)**: Provides detailed information about the log. Debugging should only be entered by qualified support personnel.

2. To delete an existing host, select the check box next to the host and click **Delete**.

3. To modify the settings for an existing host, select the check box next to the host, change the desired information, and click **Apply**.

4. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

The **Status** field in the Server Configuration table shows whether the remote logging host is currently active.
Trap Logs

Use the Trap Logs page to view information about the SNMP traps generated on the switch. To access the Trap Logs page, click the Monitoring > Logs tab, and then click the Trap Logs link.

The following table describes the Trap Log information displayed on the screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Traps Since Last Reset</td>
<td>The number of traps that have occurred since the switch last reboot.</td>
</tr>
<tr>
<td>Trap Log Capacity</td>
<td>The maximum number of traps stored in the log. If the number of traps exceeds the capacity, the entries will overwrite the oldest entries.</td>
</tr>
<tr>
<td>Number of Traps Since Log Last Viewed</td>
<td>The number of traps that have occurred since the traps were last displayed. Displaying the traps by any method (such as terminal interface display, Web display, or upload file from switch) will cause this counter to be cleared to 0.</td>
</tr>
</tbody>
</table>

The page also displays information about the traps that were sent.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log</td>
<td>The sequence number of this trap.</td>
</tr>
<tr>
<td>System Up Time</td>
<td>The time at which this trap occurred, expressed in days, hours, minutes, and seconds since the last reboot of the switch.</td>
</tr>
<tr>
<td>Trap</td>
<td>Information identifying the trap.</td>
</tr>
</tbody>
</table>
Click **Clear Counters** to clear all the counters. This resets all statistics for the trap logs to the default values.

**Event Logs**

Use the Event Log page to display the event log, which is used to hold error messages for catastrophic events. After the event is logged and the updated log is saved in flash memory, the switch will be reset. The log can hold at least 2,000 entries and is erased when an attempt is made to add an entry after it is full. The event log is preserved across system resets.

To access the Event Log page, click the Monitoring > Logs tab, and then click the Event Logs link.

The following table describes the Event Log information displayed on the screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry</td>
<td>The number of the entry within the event log. The most recent entry is first.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type of entry.</td>
</tr>
<tr>
<td>Filename</td>
<td>The GS108T or GS110TP source code filename identifying the code that detected the event.</td>
</tr>
<tr>
<td>Line</td>
<td>The line number within the source file of the code that detected the event.</td>
</tr>
<tr>
<td>Task ID</td>
<td>The OS-assigned ID of the task reporting the event.</td>
</tr>
<tr>
<td>Code</td>
<td>The event code passed to the event log handler by the code reporting the event.</td>
</tr>
<tr>
<td>Time</td>
<td>The time the event occurred, measured from the previous reset.</td>
</tr>
</tbody>
</table>

Use the buttons at the bottom of the page to perform the following actions:

- Click **Clear** to clear the messages out of the Event Log.
- Click **Refresh** to refresh the data on the screen and display the most current information.
Port Mirroring

The page under the Mirroring link allows you to view and configure port mirroring on the system.

Multiple Port Mirroring

Port mirroring selects the network traffic for analysis by a network analyzer. This is done for specific ports of the switch. As such, many switch ports are configured as source ports and one switch port is configured as a destination port. You have the ability to configure how traffic is mirrored on a source port. Packets that are received on the source port, that are transmitted on a port, or are both received and transmitted, can be mirrored to the destination port.

The packet that is copied to the destination port is in the same format as the original packet on the wire. This means that if the mirror is copying a received packet, the copied packet is VLAN tagged or untagged as it was received on the source port. If the mirror is copying a transmitted packet, the copied packet is VLAN tagged or untagged as it is being transmitted on the source port.

Use the Multiple Port Mirroring page to define port mirroring sessions.

To access the Multiple Port Mirroring page, click Monitoring > Port Mirroring.

To configure Port Mirroring:

1. Select the check box next to a port to configure it as a source port.
2. In the Destination Port field, specify the port to which port traffic is be copied. Use the g1, g2,...format to specify the port. You can configure only one destination port on the system.
3. From the **Session Mode** menu, select the mode for port mirroring on the selected port:
   - **Enable**: Multiple Port Mirroring is active on the selected port.
   - **Disable**: Port mirroring is not active on the selected port, but the mirroring information is retained.

4. Click **Apply** to apply the settings to the system. If the port is configured as a source port, the **Mirroring Port** field value is Mirrored.

5. To delete a mirrored port, select the check box next to the mirrored port, and then click **Delete**.

6. Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.
Maintaining the System

Use the features available from the Maintenance tab to help you manage the switch. The Maintenance tab contains links to the following features:

- *Reset* on page 220
- *Upload File From Switch* on page 222
- *Download File To Switch* on page 223
- *File Management* on page 228
- *Troubleshooting* on page 231
Reset

The Reset menu contains links to the following options:

- Device Reboot on page 220
- Factory Default on page 221

Device Reboot

Use the Device Reboot page to reboot the GS108T or GS110TP.

To access the Device Reboot page, click Maintenance > Reset > Device Reboot.

To reboot the switch:

1. Select the check box on the page.
2. Click Apply. The switch resets immediately. The management interface is not available until the switch completes the boot cycle. After the switch resets, the login screen appears.
Factory Default

Use the Factory Default page to reset the system configuration to the factory default values.

**Note:** If you reset the switch to the default configuration, the IP address is reset to 192.168.0.239, and the DHCP client is enabled. If you lose network connectivity after you reset the switch to the factory defaults, see *Connecting the Switch to the Network* on page 11.

To access the Factory Defaults page, click **Maintenance > Reset > Factory Default**.

To reset the switch to the factory default settings:

1. Select the check box on the page.
2. Click **Apply**. The switch resets immediately.
Upload File From Switch

Use the File Upload page to upload configuration (ASCII), log (ASCII), and image (binary) files from the switch to the TFTP server.

To display the File Upload page, click Maintenance > Upload > File Upload.

To upload a file from the switch to the TFTP server:

1. Use the File Type menu to specify the type of file you want to upload:
   - **Code**: Uploads a stored code image.
   - **Text Configuration**: Uploads the text configuration file.
   - **Error Log**: Uploads the system error (persistent) log, sometimes referred to as the event log.
   - **Buffered Log**: Uploads the system buffered (in-memory) log.
   - **Trap Log**: Uploads the system trap records.

2. If the file type is Code, specify whether to upload image1 or image2. This field is only visible when Code is selected as the File Type.

3. From the Server Address Type filed, specify the format to use for the address you type in the TFTP Server Address field:
   - **IPv4**: Indicates the TFTP server address is an IP address in dotted-decimal format.
   - **DNS**: Indicates the TFTP server address is a hostname.

4. In the Server Address field, specify the IP address or hostname of the TFTP server. The address you type must be in the format indicated by the TFTP Server Address Type.

5. In the Transfer File Path field, specify the path on the TFTP server where you want to put the file. You may enter up to 32 characters. Include the backslash at the end of the path. A path name with a space is not accepted. Leave this field blank to save the file to the root TFTP directory.
6. In the **Transfer File Name** field, specify a destination file name for the file to upload. You may enter up to 32 characters. The transfer fails if you do not specify a file name. For a code transfer, use an `.stk` file extension.

7. Select the **Start File Transfer** check box to initiate the file upload.

8. Click **Apply** to begin the file transfer.

The last row of the table displays information about the progress of the file transfer. The page refreshes automatically until the file transfer completes or fails.

### Download File To Switch

The switch supports system file downloads from a remote system to the switch by using either TFTP or HTTP.

The **Download** menu contains links to the following options:

- **TFTP File Download** on page 223
- **HTTP File Download** on page 225

### TFTP File Download

Use the Download File to Switch page to download device software, the image file, the configuration files and SSL files from a TFTP server to the switch.

You can also download files via HTTP. See **HTTP File Download** on page 225 for additional information.

To access the TFTP File Download page, click **Maintenance > Download > TFTP File Download**.
Before you download a file to the switch, the following conditions must be true:

- The file to download from the TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch has a path to the TFTP server.

To download a file to the switch from a TFTP server:

1. From the **File Type** menu, Specify what type of file you want to download to the switch:
   - **Code**: The code is the system software image, which is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy; while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non-active image. This is a safety feature for faults occurring during the boot upgrade process.
   - **Text Configuration**: A text-based configuration file enables you to edit a configured text file (startup-config) offline as needed without having to translate the contents for the switch to understand. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name, serial number, IP address), and download it to that device.
   - **Boot Code**: The boot code used to automatically boot the system. Boot code might need to be downloaded to the switch when downgrading the software image to an older version.

   **CAUTION:**
   
   Downloading boot code to the switch that is not compatible with the software image can make the switch unusable. Make sure the boot code is appropriate for the software image version before downloading the boot code.


2. If you are downloading a GS108T or GS110TP image (Code), select the image on the switch to overwrite. This field is only visible when Code is selected as the File Type.

   **Note:** It is recommended that you not overwrite the active image. The system will display a warning that you are trying to overwrite the
3. From the **Server Address Type** field, specify the format for the address you type in the TFTP Server Address field
   - **IPv4**. Indicates the TFTP server address is an IP address in dotted-decimal format.
   - **DNS**. Indicates the TFTP server address is a hostname.

4. In the **Server Address** field, specify the IP address or hostname of the TFTP server. The address you type must be in the format indicated by the TFTP Server Address Type.

5. In the **Transfer File Path** field, specify the path on the TFTP server where the file is located. You may enter up to 32 characters. Include the backslash at the end of the path. A path name with a space is not accepted. Leave this field blank to save the file to the root TFTP directory.

6. In the **Remote File Name** field, specify the name of the file to download from the TFTP server. You may enter up to 32 characters. A file name with a space is not accepted.

7. Select the **Start File Transfer** check box to initiate the file upload.

8. Click **Apply** to begin the file transfer.

   The last row of the table displays information about the progress of the file transfer. The page refreshes automatically until the file transfer completes or fails.

To activate a software image that you download to the switch, see **File Management** on page 228.

**HTTP File Download**

Use the HTTP File Download page to download files of various types to the switch using an HTTP session (for example, via your Web browser).

To display this page, click **Maintenance > Download > HTTP File Download**.

---

*Copyright © 1996–2006 Netgear®.*
To download a file to the switch from by using HTTP:

1. From the **File Type** menu, Specify what type of file you want to download to the switch:
   - **Code**: The code is the system software image, which is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy; while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non-active image. This is a safety feature for faults occurring during the boot upgrade process.
   - **Text Configuration**: A text-based configuration file enables you to edit a configured text file (startup-config) offline as needed without having to translate the contents for the switch to understand. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name, serial number, IP address), and download it to that device.
   - **Boot Code**: The boot code used to automatically boot the system. Boot code might need to be downloaded to the switch when downgrading the software image to an older version.

   **CAUTION:**
   Downloading boot code to the switch that is not compatible with the software image can make the switch unusable. Make sure the boot code is appropriate for the software image version before downloading the boot code.


2. If you are downloading a GS108T or GS110TP image (Code), select the image on the switch to overwrite. This field is only visible when Code is selected as the File Type.

   **Note**: It is recommended that you not overwrite the active image. The system will display a warning that you are trying to overwrite the active image.

3. Click **Browse** to open a file upload window to locate the file you want to download.

4. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.
5. Click the **Apply** button to initiate the file download.

---

**Note:** After a file transfer is started, please wait until the page refreshes. When the page refreshes, the *Select File* option will be blanked out. This indicates that the file transfer is done.
File Management

The system maintains two versions of the GS108T or GS110TP software in permanent storage. One image is the active image, and the second image is the backup image. The active image is loaded during subsequent switch restarts. This feature reduces switch down time when upgrading or downgrading the GS108T or GS110TP software.

The File Management menu contains links to the following options:

• Dual Image Configuration on page 228
• Dual Image Status on page 229

Dual Image Configuration

The system running a legacy software version will ignore (not load) a configuration file created by the newer software version. When a configuration file created by the newer software version is discovered by the system running an older version of the software, the system will display an appropriate warning to the user.

Use the Dual Image Configuration page to set the boot image, configure an image description, or delete an image.

To display the Dual Image Configuration page, click Maintenance > File Management > Dual Image > Dual Image Configuration.

To configure Dual Image settings:

1. Select the image to configure.
   
   The Current-active field displays the name of the active image.

2. To configure a descriptive name for the selected software image, type the name in the Image Description field.
3. To set the selected image as the active image, select the **Active Image** check box.

   **Note:** After activating an image, you must perform a system reset of the switch in order to run the new code.

4. To remove the selected image from permanent storage on the switch, select the **Delete Image** check box. You cannot delete the active image.

5. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.

6. Click **Apply** to apply the settings to the switch.

**Dual Image Status**

You can use the Dual Image Status page to view information about the system images on the device.

To display the Dual Image Status page, click **Maintenance > File Management > Dual Image > Dual Image Status.**
The following table describes the information on the Dual Image Status page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit</td>
<td>The unit ID of the switch is always 1.</td>
</tr>
<tr>
<td>Image1 Ver</td>
<td>Displays the version of the image1 code file.</td>
</tr>
<tr>
<td>Image2 Ver</td>
<td>Displays the version of the image2 code file.</td>
</tr>
<tr>
<td>Current-active</td>
<td>Displays the currently active image on this switch.</td>
</tr>
<tr>
<td>Next-active</td>
<td>Displays the image to be used on the next restart of this switch.</td>
</tr>
<tr>
<td>Image1 Description</td>
<td>Displays the description associated with the image1 code file.</td>
</tr>
<tr>
<td>Image2 Description</td>
<td>Displays the description associated with the image2 code file.</td>
</tr>
</tbody>
</table>

Click **Refresh** to display the latest information from the switch.

For information about how to update or change the system images, see *File Management* on page 228.
Troubleshooting

The Troubleshooting menu contains links to the following options:

- Ping on page 231
- Traceroute on page 232

Ping

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

To access the Ping page, click Maintenance > Troubleshooting > Ping.

To configure the settings and ping a host on the network:

1. In the Hostname/IP Address field, specify the IP address or the hostname of the station you want the switch to ping. The initial value is blank. This information is not retained across a power cycle.

2. Optionally, configure the following settings:
   - Count. Specify the number of pings to send. The valid range is 1–15.
   - Interval. Specify the number of seconds between pings sent. The valid range is 1–60.
   - Size. Specify the size of the ping (ICMP) packet to send. The valid range is 0–65507.

3. Click Cancel to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.
4. Click **Apply** to send the ping. The switch sends the number of pings specified in the **Count** field, and the results are displayed below the configurable data in the **Ping** area.

   - If successful, you will see “Reply From IP/Host: icmp_seq = 0. time = xx usec. Tx = x, Rx = x Min/Max/Avg RTT = x/x/x msec.”
   - If a reply to the ping is not received, you will see “Reply From IP/Host: Destination Unreachable. Tx = x, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec”.

**Traceroute**

Use the Traceroute utility to discover the paths that a packet takes to a remote destination.

To display this page, click **Maintenance > Troubleshooting > Traceroute**.

To configure the Traceroute settings and send probe packets to discover the route to a host on the network:

1. In the **Hostname/IP Address** field, specify the IP address or the hostname of the station you want the switch to ping. The initial value is blank. This information is not retained across a power cycle.
2. Optionally, configure the following settings:
   - **Probes Per Hop**. Specify the number of times each hop should be probed. The valid range is 1–10.
   - **MaxTTL**. Specify the maximum time-to-live for a packet in number of hops. The valid range is 1–255.
   - **InitTTL**. Specify the initial time-to-live for a packet in number of hops. The valid range is 0–255.
• **MaxFail.** Specify the maximum number of failures allowed in the session. The valid range is 0–255.

• **Interval.** Specify the time between probes in seconds. The valid range is 1–60.

• **Port.** Specify the UDP destination port in probe packets. The valid range is 1–65535.

• **Size.** Specify the size of probe packets. The valid range is 0–65507.

3. Click **Cancel** to cancel the operation on the screen and reset the data on the screen to the latest value of the switch.

4. Click **Apply** to initiate the traceroute. The results display in the TraceRoute area.
Accessing Help

Use the features available from the Help tab to connect to online resources for assistance. The Help tab contains a link to Online Help.

Online Help

The Online Help includes the following pages:

- Support on page 235
- User Guide on page 236

Support

Use the Support page to connect to the Online Support site at netgear.com.

To access the Support page, click Help > Support.

To connect to the NETGEAR support site for the GS108T or GS110TP, click Apply.
User Guide

Use the User Guide page to access the GS108T and GS110TP Smart Switch Software Administration Manual (the guide you are now reading) that is available on the NETGEAR Website.

To access the User Guide page, click Help > User Guide.

To access to the User Guide that is available online, click Apply.
Appendix A: Hardware Specifications and Default Values

GS108T and GS110TP Gigabit Smart Switches Specifications

The GS108T and GS110TP Gigabit Smart Switches conform to the TCP/IP, UDP, HTTP, ICMP, TFTP, DHCP, IEEE 802.1D, IEEE 802.1p, and IEEE 802.1Q standards.

GS108 Specifications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>Eight 10/100/1000 Ethernet ports</td>
</tr>
<tr>
<td>PoE</td>
<td>PoE-Powered Device</td>
</tr>
<tr>
<td>Flash memory size</td>
<td>16 MB</td>
</tr>
<tr>
<td>SRAM size and type</td>
<td>64 MB DDR</td>
</tr>
</tbody>
</table>

GS110 Specifications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>Eight 10/100/1000 Ethernet ports</td>
</tr>
<tr>
<td></td>
<td>Two 1000M SFP Gigabit Ethernet ports</td>
</tr>
<tr>
<td>PoE</td>
<td>Ports 1–8, IEEE 802.3af, Alternative A (MDI-X)</td>
</tr>
<tr>
<td>Flash memory size</td>
<td>16 MB</td>
</tr>
<tr>
<td>SRAM size and type</td>
<td>64 MB DDR</td>
</tr>
</tbody>
</table>
GS108T and GS110TP Switch Performance

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switching capacity</td>
<td>Non-Blocking Full WireSpeed on all packet sizes</td>
</tr>
<tr>
<td>Forwarding method</td>
<td>Store and Forward</td>
</tr>
<tr>
<td>Packet forwarding rate</td>
<td>10M:14,880 pps/100M:148,810 pps/1G:1,488,000 pps</td>
</tr>
<tr>
<td>MAC addresses</td>
<td>4K</td>
</tr>
<tr>
<td>Green Ethernet</td>
<td>Power consumption savings by cable length (&lt;10m)</td>
</tr>
<tr>
<td></td>
<td>Automatic power down on port when link is down (GS110TP only)</td>
</tr>
</tbody>
</table>

GS108T and GS110TP Switch Features and Defaults

Port Characteristics

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto negotiation/static speed/duplex</td>
<td>All ports</td>
<td>Auto negotiation</td>
</tr>
<tr>
<td>Auto MDI/MDIX</td>
<td>N/A</td>
<td>Enabled</td>
</tr>
<tr>
<td>802.3x flow control/back pressure</td>
<td>1 (per system)</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port mirroring</td>
<td>1</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port trunking (aggregation)</td>
<td>4</td>
<td>Pre-configured</td>
</tr>
<tr>
<td>802.1D spanning tree</td>
<td>1</td>
<td>Disabled</td>
</tr>
<tr>
<td>802.1w RSTP</td>
<td>1</td>
<td>Disabled</td>
</tr>
<tr>
<td>802.1s spanning tree</td>
<td>3 instances</td>
<td>Disabled</td>
</tr>
<tr>
<td>Static 802.1Q tagging</td>
<td>64</td>
<td>VID = 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Member ports = 8 (GS108T)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Member ports = 10 (GS110TP)</td>
</tr>
<tr>
<td>Learning process</td>
<td>Supports Static and dynamic MAC entries</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dynamic learning is enabled by default</td>
<td></td>
</tr>
<tr>
<td>PoE (GS110TP only)</td>
<td>8</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
## Traffic Control

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storm control</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td>Jumbo frame</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max = 9216 bytes</td>
</tr>
</tbody>
</table>

## Quality Of Service

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of queues</td>
<td>4</td>
<td>N/A</td>
</tr>
<tr>
<td>Port based</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>802.1p</td>
<td>1</td>
<td>Enabled</td>
</tr>
<tr>
<td>DSCP</td>
<td>1</td>
<td>Disabled</td>
</tr>
<tr>
<td>Rate limiting</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td>Auto-QoS</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

## Security

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td>MAC ACL</td>
<td>100 (Shared with IP ACL)</td>
<td>All MAC addresses allowed</td>
</tr>
<tr>
<td>IP access list</td>
<td>100 (shared with MACACL)</td>
<td>All IP addresses allowed</td>
</tr>
<tr>
<td>Password control access</td>
<td>1</td>
<td>Idle timeout = 5 mins. Password = &quot;password&quot;</td>
</tr>
<tr>
<td>Management security</td>
<td>1 profile with 20 rules for HTTP/HTTPS/SNMP access to allow/deny an IP address/subnet</td>
<td>All IP addresses allowed</td>
</tr>
<tr>
<td>Port MAC lock down</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
# System Setup

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot code update</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>DHCP/manual IP</td>
<td>1</td>
<td>DHCP enabled/192.168.0.239</td>
</tr>
<tr>
<td>Default gateway</td>
<td>1</td>
<td>192.168.0.254</td>
</tr>
<tr>
<td>System name configuration</td>
<td>1</td>
<td>NULL</td>
</tr>
<tr>
<td>Configuration save/restore</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>Firmware upgrade</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>Restore defaults</td>
<td>1 (Web and front-panel button)</td>
<td>N/A</td>
</tr>
<tr>
<td>Dual image support</td>
<td>1</td>
<td>Enabled</td>
</tr>
<tr>
<td>Factory reset</td>
<td>1</td>
<td>N/A</td>
</tr>
</tbody>
</table>

# Management

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-session Web connections</td>
<td>16</td>
<td>Enabled</td>
</tr>
<tr>
<td>SNMPv1/V2c</td>
<td>Max 5 community entries</td>
<td>Enabled (read, read-write communities)</td>
</tr>
<tr>
<td>SNMP v3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time control</td>
<td>1 (Local or SNTP)</td>
<td>Local Time enabled</td>
</tr>
<tr>
<td>LLDP/LLDP-MED</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td>Logging</td>
<td>3 (Memory/Flash/Server)</td>
<td>Memory Log enabled</td>
</tr>
<tr>
<td>MIB support</td>
<td>1</td>
<td>Disabled</td>
</tr>
<tr>
<td>Smart Control Center</td>
<td>N/A</td>
<td>Enabled</td>
</tr>
<tr>
<td>Statistics</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## Other Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP snooping v1/v2</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td>Configurations upload/download</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>EAPoL flooding</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td>BPDU flooding</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td>Static multicast groups</td>
<td>8</td>
<td>Disabled</td>
</tr>
<tr>
<td>Filter multicast control</td>
<td>1</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
This chapter contains information about how to configure the following features:

- *Virtual Local Area Networks (VLANs)* on page 244
- *Access Control Lists (ACLs)* on page 246
- *Differentiated Services (DiffServ)* on page 249
- *802.1X* on page 254
- *MSTP* on page 257
Virtual Local Area Networks (VLANs)

A local area network (LAN) can generally be defined as a broadcast domain. Hubs, bridges, or switches in the same physical segment or segments connect all end node devices. End nodes can communicate with each other without the need for a router. Routers connect LANs together, routing the traffic to the appropriate port.

A virtual LAN (VLAN) is a local area network with a definition that maps workstations on some basis other than geographic location (for example, by department, type of user, or primary application). To enable traffic to flow between VLANs, traffic must go through a router, just as if the VLANs were on two separate LANs.

A VLAN is a group of PCs, servers, and other network resources that behave as if they were connected to a single network segment—even though they might not be. For example, all marketing personnel might be spread throughout a building. Yet if they are all assigned to a single VLAN, they can share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specified individuals, depending on how the IT manager has set up the VLANs.

VLANs have a number of advantages:

- It is easy to do network segmentation. Users that communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group’s traffic is contained largely within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.
- They are easy to manage. The addition of nodes, as well as moves and other changes, can be dealt with quickly and conveniently from a management interface rather than from the wiring closet.
- They provide increased performance. VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.
- They ensure enhanced network security. VLANs create virtual boundaries that can be crossed only through a router. So standard, router-based security measures can be used to restrict access to each VLAN.

Packets received by the switch are treated in the following way:

- When an untagged packet enters a port, it is automatically tagged with the port’s default VLAN ID tag number. Each port has a default VLAN ID setting that is user configurable (the default setting is 1). The default VLAN ID setting for each port can be changed in the Port PVID Configuration screen. See Port VLAN ID Configuration on page 87.
- When a tagged packet enters a port, the tag for that packet is unaffected by the default VLAN ID setting. The packet proceeds to the VLAN specified by its VLAN ID tag number.
- If the port through which the packet entered does not have membership with the VLAN specified by the VLAN ID tag, the packet is dropped.
- If the port is a member of the VLAN specified by the packet’s VLAN ID, the packet can be sent to other ports with the same VLAN ID.
• Packets leaving the switch are either tagged or untagged, depending on the setting for that port’s VLAN membership properties. A U for a given port means that packets leaving the switch from that port are untagged. Inversely, a T for a given port means that packets leaving the switch from that port are tagged with the VLAN ID that is associated with the port.

The example given in this section comprises numerous steps to illustrate a wide range of configurations to help provide an understanding of tagged VLANs.

**VLAN Example Configuration**

This example demonstrates several scenarios of VLAN use and describes how the switch handles tagged and untagged traffic.

In this example, you create two new VLANs, change the port membership for default VLAN 1, and assign port members to the two new VLANs:

1. In the Basic VLAN Configuration screen (see VLAN Configuration on page 84), create the following VLANs:
   - A VLAN with VLAN ID 10.
   - A VLAN with VLAN ID 20.

2. In the VLAN Membership screen (see VLAN Membership Configuration on page 86) specify the VLAN membership as follows:
   - For the default VLAN with VLAN ID 1, specify the following members: port 7 (U) and port 8 (U).
   - For the VLAN with VLAN ID 10, specify the following members: port 1 (U), port 2 (U), and port 3 (T).
   - For the VLAN with VLAN ID 20, specify the following members: port 4 (U), port 5 (T), and port 6 (U).

3. In the Port PVID Configuration screen (see Port VLAN ID Configuration on page 87), specify the PVID for ports g1 and g4 so that packets entering these ports are tagged with the port VLAN ID:
   - Port g1: PVID 10
   - Port g4: PVID 20

4. With the VLAN configuration that you set up, the following situations produce results as described:
   - If an untagged packet enters port 1, the switch tags it with VLAN ID 10. The packet has access to port 2 and port 3. The outgoing packet is stripped of its tag to leave port 2 as an untagged packet. For port 3, the outgoing packet leaves as a tagged packet with VLAN ID 10.
   - If a tagged packet with VLAN ID 10 enters port 3, the packet has access to port 1 and port 2. If the packet leaves port 1 or port 2, it is stripped of its tag to leave the switch as an untagged packet.
   - If an untagged packet enters port 4, the switch tags it with VLAN ID 20. The packet has access to port 5 and port 6. The outgoing packet is stripped of its tag to become an untagged packet as it leaves port 6. For port 5, the outgoing packet leaves as a tagged packet with VLAN ID 20.
Access Control Lists (ACLs)

ACLs ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.

ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and provide security for the network. ACLs are normally used in firewall routers that are positioned between the internal network and an external network, such as the Internet. They can also be used on a router positioned between two parts of the network to control the traffic entering or exiting a specific part of the internal network. The added packet processing required by the ACL feature does not affect switch performance. That is, ACL processing occurs at wire speed.

Access lists are a sequential collection of permit and deny conditions. This collection of conditions, known as the filtering criteria, is applied to each packet that is processed by the switch or the router. The forwarding or dropping of a packet is based on whether or not the packet matches the specified criteria.

Traffic filtering requires the following two basic steps:

1. Create an access list definition.

   The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. Additionally, you can assign traffic that matches the criteria to a particular queue or redirect the traffic to a particular port. A default deny all rule is the last rule of every list.

2. Apply the access list to an interface in the inbound direction.

GS108T and GS110TP Smart Switches allow ACLs to be bound to physical ports and LAGs. The switch software supports MAC ACLs and IP ACLs.

MAC ACL Example Configuration

The following example shows how to create a MAC-based ACL that permits Ethernet traffic from the Sales department on specified ports and denies all other traffic on those ports.

1. From the MAC ACL screen, create an ACL with the name Sales_ACL for the Sales department of your network (See MAC ACL on page 182).

   By default, this ACL will be bound on the inbound direction, which means the switch will examine traffic as it enters the port.

2. From the MAC Rules screen, create a rule for the Sales_ACL with the following settings:
   - ID: 1
   - Action: Permit
   - Assign Queue: 0
   - Match Every: False
   - CoS: 0
   - Destination MAC: 01:02:1A:BC:DE:EF
• Destination MAC Mask: 00:00:00:FF:FF
• Source MAC: 02:02:1A:BC:DE:EF
• Source MAC Mask: 00:00:00:FF:FF
• VLAN ID: 2

For more information about MAC ACL rules, see MAC Rules on page 183.

3. From the MAC Binding Configuration screen, assign the Sales_ACL to the interface gigabit ports 6, 7, and 8, and then click Apply (See MAC Binding Configuration on page 184).

You can assign an optional sequence number to indicate the order of this access list relative to other access lists if any are already assigned to this interface and direction.

4. The MAC Binding Table displays the interface and MAC ACL binding information (See MAC Binding Table on page 186).

The ACL named Sales_ACL looks for Ethernet frames with destination and source MAC addresses and MAC masks defined in the rule. Also, the frame must be tagged with VLAN ID 2, which is the Sales department VLAN. The CoS value of the frame must be 0, which is the default value for Ethernet frames. Frames that match this criteria are permitted on interfaces 6, 7, and 8 and are assigned to the hardware egress queue 0, which is the default queue. All other traffic is explicitly denied on these interfaces. To allow additional traffic to enter these ports, you must add a new permit rule with the desired match criteria and bind the rule to interfaces 6, 7, and 8.
Standard IP ACL Example Configuration

The following example shows how to create an IP-based ACL that prevents any IP traffic from the Finance department from being allowed on the ports that are associated with other departments. Traffic from the Finance department is identified by each packet’s network IP address.

1. From the IP ACL screen, create a new IP ACL with an IP ACL ID of 1 (See IP ACL on page 187).
2. From the IP Rules screen, create a rule for IP ACL 1 with the following settings:
   • Rule ID: 1
   • Action: Deny
   • Assign Queue ID: 0 (optional: 0 is the default value)
   • Match Every: False
   • Source IP Address: 192.168.187.0
   • Source IP Mask: 255.255.255.0

For additional information about IP ACL rules, see IP Rules on page 188.

3. Click Add.
4. From the IP Rules screen, create a second rule for IP ACL 1 with the following settings:
   • Rule ID: 2
   • Action: Permit
   • Match Every: True

5. Click Add.
6. From the IP Binding Configuration page, assign ACL ID 1 to the interface gigabit ports 2, 3, and 4, and assign a sequence number of 1 (See IP Binding Configuration on page 193).

   By default, this IP ACL is bound on the inbound direction, so it examines traffic as it enters the switch.

7. Click Apply.
8. Use the IP Binding Table screen to view the interfaces and IP ACL binding information (See IP Binding Table on page 194).

The IP ACL in this example matches all packets with the source IP address and subnet mask of the Finance department’s network and deny it on the Ethernet interfaces 2, 3, and 4 of the switch. The second rule permits all non-Finance traffic on the ports. The second rule is required because there is an explicit deny all rule as the lowest priority rule.
Differentiated Services (DiffServ)

Standard IP-based networks are designed to provide best effort data delivery service. Best effort service implies that the network deliver the data in a timely fashion, although there is no guarantee that it will. During times of congestion, packets may be delayed, sent sporadically, or dropped. For typical Internet applications, such as e-mail and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. However, any degradation of service has undesirable effects on applications with strict timing requirements, such as voice or multimedia.

Quality of Service (QoS) can provide consistent, predictable data delivery by distinguishing between packets that have strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given special treatment in a QoS-capable network. With this in mind, all elements of the network must be QoS-capable. If one node is unable to meet the necessary timing requirements, this creates a deficiency in the network path and the performance of the entire packet flow is compromised.

There are two basic types of QoS:

- **Integrated Services**: network resources are apportioned based on request and are reserved (resource reservation) according to network management policy (RSVP, for example).
- **Differentiated Services**: network resources are apportioned based on traffic classification and priority, giving preferential treatment to data with strict timing requirements.

switch switches support DiffServ.

The DiffServ feature contains a number of conceptual QoS building blocks you can use to construct a differentiated service network. Use these same blocks in different ways to build other types of QoS architectures.

There are 3 key QoS building blocks needed to configure DiffServ:

- Class
- Policy
- Service (i.e., the assignment of a policy to a directional interface)

**Class**

You can classify incoming packets at layers 2, 3 and 4 by inspecting the following information for a packet:

- Source/destination MAC address
- EtherType
- Class of Service (802.1p priority) value (first/only VLAN tag)
- VLAN ID range (first/only VLAN tag)
- Secondary 802.1p priority value (second/inner VLAN tag)
- Secondary VLAN ID range (second/inner VLAN tag)
• IP Service Type octet (also known as: ToS bits, Precedence value, DSCP value)
• Layer 4 protocol (TCP, UDP etc.)
• Layer 4 source/destination ports
• Source/destination IP address

From a DiffServ point of view, there are two types of classes:

• DiffServ traffic classes
• DiffServ service levels/forwarding classes

**DiffServ Traffic Classes**

With DiffServ, you define which traffic classes to track on an ingress interface. You can define simple BA classifiers (DSCP) and a wide variety of multi-field (MF) classifiers:

• Layer 2; Layers 3, 4 (IP only)
• Protocol-based
• Address-based

You can combine these classifiers with logical AND or OR operations to build complex MF-classifiers (by specifying a class type of all or any, respectively). That is, within a single class, multiple match criteria are grouped together as an AND expression or a sequential OR expression, depending on the defined class type. Only classes of the same type can be nested; class nesting does not allow for the negation (i.e., exclude option) of the referenced class.

To configure DiffServ, you must define service levels, namely the forwarding classes/PHBs identified by a given DSCP value, on the egress interface. These service levels are defined by configuring BA classes for each.

**Creating Policies**

Use DiffServ policies to associate a collection of classes that you configure with one or more QoS policy statements. The result of this association is referred to as a policy.

From a DiffServ perspective, there are two types of policies:

• **Traffic Conditioning Policy**: a policy applied to a DiffServ traffic class
• **Service Provisioning Policy**: a policy applied to a DiffServ service level

You must manually configure the various statements and rules used in the traffic conditioning and service provisioning policies to achieve the desired Traffic Conditioning Specification (TCS) and the Service Level Specification (SLS) operation, respectively.
Traffic Conditioning Policy

Traffic conditioning pertains to actions performed on incoming traffic. There are several distinct QoS actions associated with traffic conditioning:

- **Dropping**: drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.

- **Marking IP DSCP or IP Precedence**: marking/re-marking the DiffServ code point in a packet with the DSCP value representing the service level associated with a particular DiffServ traffic class. Alternatively, the IP Precedence value of the packet can be marked/re-marked.

- **Marking CoS (802.1p)**: sets the three-bit priority field in the first/only 802.1p header to a specified value when packets are transmitted for the traffic class. An 802.1p header is inserted if it does not already exist. This is useful for assigning a layer 2 priority level based on a DiffServ forwarding class (i.e., DSCP or IP Precedence value) definition to convey some QoS characteristics to downstream switches which do not routinely look at the DSCP value in the IP header.

- **Policing**: a method of constraining incoming traffic associated with a particular class so that it conforms to the terms of the TCS. Special treatment can be applied to out-of-profile packets that are either in excess of the conformance specification or are non-conformant. The DiffServ feature supports the following types of traffic policing treatments (actions):
  - drop: the packet is dropped
  - mark cos: the 802.1p user priority bits are (re)marked and forwarded
  - mark dscp: the packet DSCP is (re)marked and forwarded
  - mark prec: the packet IP Precedence is (re)marked and forwarded
  - send: the packet is forwarded without DiffServ modification

  Color Mode Awareness: Policing in the DiffServ feature uses either color blind or color aware mode. Color blind mode ignores the coloration (marking) of the incoming packet. Color aware mode takes into consideration the current packet marking when determining the policing outcome. An auxiliary traffic class is used in conjunction with the policing definition to specify a value for one of the 802.1p, Secondary 802.1p, IP DSCP, or IP Precedence fields designating the incoming color value to be used as the conforming color. The color of exceeding traffic may be optionally specified as well.

- **Counting**: updating octet and packet statistics to keep track of data handling along traffic paths within DiffServ. In this DiffServ feature, counters are not explicitly configured by the user, but are designed into the system based on the DiffServ policy being created. See the Statistics section of this document for more details.

- **Assigning QoS Queue**: directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.

- **Redirecting**: forces classified traffic stream to a specified egress port (physical or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.
DiffServ Example Configuration

To create a DiffServ Class/Policy and attach it to a switch interface, follow these steps:

1. From the QoS Class Configuration screen, create a new class with the following settings:
   • Class Name: Class1
   • Class Type: All
   For more information about this screen, see Class Configuration on page 135.

2. Click the Class1 hyperlink to view the DiffServ Class Configuration screen for this class.

3. Configure the following settings for Class1:
   • Protocol Type: UDP
   • Source IP Address: 192.12.1.0
   • Source Mask: 255.255.255.0
   • Source L4 Port: Other, and enter 4567 as the source port value
   • Destination IP Address: 192.12.2.0
   • Destination Mask: 255.255.255.0
   • Destination L4 Port: Other, and enter 4568 as the destination port value
   For more information about this screen, see Class Configuration on page 135.

4. Click Apply.

5. From the Policy Configuration screen, create a new policy with the following settings:
   • Policy Selector: Policy1
   • Member Class: Class1
   For more information about this screen, see Policy Configuration on page 138.

6. Click Add to add the new policy.

7. Click the Policy1 hyperlink to view the Policy Class Configuration screen for this policy.

8. Configure the Policy attributes as follows:
   • Assign Queue: 3
   • Policy Attribute: Simple Policy
   • Color Mode: Color Blind
   • Committed Rate: 1000000 Kbps
   • Committed Burst Size: 128 KB
   • Confirm Action: Send
   • Violate Action: Drop
   For more information about this screen, see Policy Configuration on page 138.

9. From the Service Configuration screen, select the check box next to interfaces g7 and g8 to attach the policy to these interfaces, and then click Apply (See Service Configuration on page 142).
All UDP packet flows destined to the 192.12.2.0 network with an IP source address from the 192.12.1.0 network that have a Layer 4 Source port of 4567 and Destination port of 4568 from this switch on ports 7 and 8 are assigned to hardware queue 3.

On this network, traffic from streaming applications uses UDP port 4567 as the source and 4568 as the destination. This real-time traffic is time sensitive, so it is assigned to a high-priority hardware queue. By default, data traffic uses hardware queue 0, which is designated as a best-effort queue.

Also the confirmed action on this flow is to send the packets with a committed rate of 1000000 Kbps and burst size of 128 KB. Packets that violate the committed rate and burst size are dropped.
802.1X

Local Area Networks (LANs) are often deployed in environments that permit unauthorized devices to be physically attached to the LAN infrastructure, or permit unauthorized users to attempt to access the LAN through equipment already attached. In such environments, it may be desirable to restrict access to the services offered by the LAN to those users and devices that are permitted to use those services.

Port-based network access control makes use of the physical characteristics of LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics and of preventing access to that port in cases in which the authentication and authorization process fails. In this context, a port is a single point of attachment to the LAN, such as ports of MAC bridges and associations between stations or access points in IEEE 802.11 Wireless LANs.

The IEEE 802.11 standard describes an architectural framework within which authentication and consequent actions take place. It also establishes the requirements for a protocol between the authenticator (the system that passes an authentication request to the authentication server) and the supplicant (the system that requests authentication), as well as between the authenticator and the authentication server.

The switch switches support a guest VLAN, which allows unauthenticated users to have limited access to the network resources.

---

**Note:** You can use QoS features to provide rate limiting on the guest VLAN to limit the network resources the guest VLAN provides.

Another 802.1X feature is the ability to configure a port to Enable/Disable EAPoL packet forwarding support. You can disable or enable the forwarding of EAPoL when 802.1X is disabled on the device.

The ports of an 802.1X authenticator switch provide the means in which it can offer services to other systems reachable via the LAN. Port-based network access control allows the operation of a switch’s ports to be controlled in order to ensure that access to its services is only permitted by systems that are authorized to do so.

Port access control provides a means of preventing unauthorized access by supplicants to the services offered by a system. Control over the access to a switch and the LAN to which it is connected can be desirable in order to restrict access to publicly accessible bridge ports or to restrict access to departmental LANs.

Access control is achieved by enforcing authentication of supplicants that are attached to an authenticator’s controlled ports. The result of the authentication process determines whether the supplicant is authorized to access services on that controlled port.
A Port Access Entity (PAE) is able to adopt one of two distinct roles within an access control interaction:

1. **Authenticator**: A Port that enforces authentication before allowing access to services available via that Port.
2. **Supplicant**: A Port that attempts to access services offered by the Authenticator.

Additionally, there exists a third role:

3. **Authentication server**: Performs the authentication function necessary to check the credentials of the Supplicant on behalf of the Authenticator.

All three roles are required in order to complete an authentication exchange.

switch switches support the Authenticator role only, in which the PAE is responsible for communicating with the Supplicant. The Authenticator PAE is also responsible for submitting the information received from the Supplicant to the Authentication Server in order for the credentials to be checked, which will determine the authorization state of the Port. The Authenticator PAE controls the authorized/unauthorized state of the controlled Port depending on the outcome of the RADIUS-based authentication process.

**802.1X Example Configuration**

This example shows how to configure the switch so that 802.1X-based authentication is required on the ports in a corporate conference room (g5–g8). These ports are available to visitors and need to be authenticated before granting access to the network. The authentication is handled by an external RADIUS server. When the visitor is successfully authenticated, traffic is automatically assigned to the guest VLAN. This example assumes that a VLAN has been configured with a VLAN ID of 150 and VLAN Name of Guest.

1. From the Port Authentication screen, select ports g5, g6, g7, and g8.
2. From the Port Control menu, select Unauthorized.

   The Port Control setting for all other ports where authentication is not needed should Authorized. When the Port Control setting is Authorized, the port is unconditionally put in a force-Authorized state and does not require any authentication. When the Port Control setting is Auto, the authenticator PAE sets the controlled port mode
3. In the Guest VLAN field for ports g5–g8, enter 150 to assign these ports to the guest VLAN. You can configure additional settings to control access to the network through the ports. See Port Security Interface Configuration on page 176 for information about the settings.

4. Click Apply.

5. From the 802.1X Configuration screen, set the Port Based Authentication State and Guest VLAN Mode to Enable, and then click Apply (See Port Security Configuration on page 175).

This example uses the default values for the port authentication settings, but there are several additional settings that you can configure. For example, the EAPOL Flood Mode field allows you to enable the forwarding of EAPoL frames when 802.1X is disabled on the device.

6. From the RADIUS Server Configuration screen, configure a RADIUS server with the following settings:
   - Server Address: 192.168.10.23
   - Secret Configured: Yes
   - Secret: secret123
   - Active: Primary

   For more information, see RADIUS Configuration on page 147.

7. Click Add.

8. From the Authentication List screen, configure the default List to use RADIUS as the first authentication method (See Authentication List Configuration on page 155).

This example enables 802.1X-based port security on the GS108T or GS110TP switch and prompts the hosts connected on ports g5-g8 for an 802.1X-based authentication. The switch passes the authentication information to the configured RADIUS server.
MSTP

Spanning Tree Protocol (STP) runs on bridged networks to help eliminate loops. If a bridge loop occurs, the network can become flooded with traffic. IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) supports multiple instances of Spanning Tree to efficiently channel VLAN traffic over different interfaces. Each instance of the Spanning Tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree, with slight modifications in the working but not the end effect (chief among the effects is the rapid transitioning of the port to the Forwarding state).

The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to the Forwarding state and the suppression of Topology Change Notification. These features are represented by the parameters pointtopoint and edgeport. MSTP is compatible to both RSTP and STP. It behaves appropriately to STP and RSTP bridges.

A MSTP bridge can be configured to behave entirely as a RSTP bridge or a STP bridge. So, an IEEE 802.1s bridge inherently also supports IEEE 802.1w and IEEE 802.1D.

The MSTP algorithm and protocol provides simple and full connectivity for frames assigned to any given VLAN throughout a Bridged LAN comprising arbitrarily interconnected networking devices, each operating MSTP, STP or RSTP. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) Regions composed of LANs and or MSTP Bridges. These Regions and the other Bridges and LANs are connected into a single Common Spanning Tree (CST). [IEEE DRAFT P802.1s/D13]

MSTP connects all Bridges and LANs with a single Common and Internal Spanning Tree (CIST). The CIST supports the automatic determination of each MST region, choosing its maximum possible extent. The connectivity calculated for the CIST provides the CST for interconnecting these Regions, and an Internal Spanning Tree (IST) within each Region. MSTP ensures that frames with a given VLAN ID are assigned to one and only one of the MSTIs or the IST within the Region, that the assignment is consistent among all the networking devices in the Region and that the stable connectivity of each MSTI and IST at the boundary of the Region matches that of the CST. The stable active topology of the Bridged LAN with respect to frames consistently classified as belonging to any given VLAN thus simply and fully connects all LANs and networking devices throughout the network, though frames belonging to different VLANs can take different paths within any Region, per IEEE DRAFT P802.1s/D13.

All bridges, whether they use STP, RSTP or MSTP, send information in configuration messages via Bridge Protocol Data Units (BPDUs) to assign port roles that determine each port’s participation in a fully and simply connected active topology based on one or more spanning trees. The information communicated is known as the spanning tree priority vector. The BPDU structure for each of these different protocols is different. A MSTP bridge will transmit the appropriate BPDU depending on the received type of BPDU from a particular port.
An MST Region comprises of one or more MSTP Bridges with the same MST Configuration Identifier, using the same MSTIs, and which have no Bridges attached that cannot receive and transmit MSTP BPDUs. The MST Configuration Identifier has the following components:

1. Configuration Identifier Format Selector
2. Configuration Name
3. Configuration Revision Level
4. Configuration Digest: 16-byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID to MSTID mapping)

As there are Multiple Instances of Spanning Tree, there is a MSTP state maintained on a per-port, per-instance basis (or on a per port per VLAN basis: as any VLAN can be in one and only one MISTI or CIST). For example, port A can be forwarding for instance 1 while discarding for instance 2. The port states have changed since IEEE 802.1D specification.

To support multiple spanning trees, a MSTP bridge has to be configured with an unambiguous assignment of VLAN IDs (VIDs) to spanning trees. This is achieved by:

1. Ensuring that the allocation of VIDs to FIDs is unambiguous.
2. Ensuring that each FID supported by the Bridge is allocated to exactly one Spanning Tree Instance.

The combination of VID to FID and then FID to MSTI allocation defines a mapping of VIDs to spanning tree instances, represented by the MST Configuration Table.

With this allocation we ensure that every VLAN is assigned to one and only one MISTI. The CIST is also an instance of spanning tree with a MSTID of 0.

An instance may occur that has no VIDs allocated to it, but every VLAN must be allocated to one of the other instances of spanning tree.

The portion of the active topology of the network that connects any two bridges in the same MST Region traverses only MST bridges and LANs in that region, and never Bridges of any kind outside the Region, in other words connectivity within the region is independent of external connectivity.

MSTP Example Configuration

This example shows how to create an MSTP instance from the GS108T or GS110TP switch. The example network has three different GS108T or GS110TP switches that serve different locations in the network. In this example, ports g1–g5 are connected to host stations, so those links are not subject to network loops. Ports g6-g8 are connected across switches 1, 2 and 3.
Perform the following procedures on each switch to configure MSTP:

1. Use the VLAN Configuration screen to create VLANs 300 and 500 (see VLAN Configuration on page 84).

2. Use the VLAN Membership screen to include ports g1–g8 as tagged (T) or untagged (U) members of VLAN 300 and VLAN 500 (see VLAN Membership Configuration on page 86).

3. From the STP Configuration screen, enable the Spanning Tree State option (see STP Switch Configuration on page 95).

   Use the default values for the rest of the STP configuration settings. By default, the STP Operation Mode is MSTP and the Configuration Name is the switch MAC address.

4. From the CST Configuration screen, set the Bridge Priority value for each of the three switches to force Switch 1 to be the root bridge:
   - Switch 1: 4096
   - Switch 2: 12288
   - Switch 3: 20480

   **Note:** Bridge priority values are multiples of 4096.

5. From the CST Port Configuration screen, select ports g1–g8 and select Enable from the STP Status menu (see CST Port Configuration on page 98).

6. Click **Apply**.

7. Select ports g1–g5 (edge ports), and select Enable from the Fast Link menu.
Since the edge ports are not at risk for network loops, ports with Fast Link enabled transition directly to the Forwarding state.

8. Click **Apply**.
   
   You can use the CST Port Status screen to view spanning tree information about each port.

9. From the MST Configuration screen, create a MST instances with the following settings:
   - MST ID: 1
   - Priority: Use the default (32768)
   - VLAN ID: 300
   
   For more information, see *MST Configuration* on page 102.

10. Click **Add**.

11. Create a second MST instance with the following settings
    - MST ID: 2
    - Priority: 49152
    - VLAN ID: 500

12. Click **Add**.

In this example, assume that Switch 1 has become the Root bridge for the MST instance 1, and Switch 2 has become the Root bridge for MST instance 2. Switch 3 has hosts in the Sales department (ports g1, g2, and g3) and in the HR department (ports g4 and g5). Switches 1 and 2 also have hosts in the Sales and Human Resources departments. The hosts connected from Switch 2 use VLAN 500, MST instance 2 to communicate with the hosts on Switch 3 directly. Likewise, hosts of Switch 1 use VLAN 300, MST instance 1 to communicate with the hosts on Switch 3 directly.

The hosts use different instances of MSTP to effectively use the links across the switch. The same concept can be extended to other switches and more instances of MSTP.
Notification of Compliance

NETGEAR Wired Products

Certificate of the Manufacturer/Importer
It is hereby certified that the NETGEAR® GS108T and GS110TP Smart Switches has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

The Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Voluntary Control Council for Interference (VCCI) Statement
This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas. When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

FCC Caution
• Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
• This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Regulatory Compliance Information
This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

Note: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.
Europe – EU Declaration of Conformity

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:
EN300 328, EN301 489-17, EN60950

For complete DoC please visit the NETGEAR EU Declarations of Conformity website at:
http://kb.netgear.com/app/answers/detail/a_id/11621/

EDOC in Languages of the European Community

<table>
<thead>
<tr>
<th>Language</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cesky [Czech]</td>
<td>NETGEAR Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími příslušnými ustanoveními smernice 1999/5/ES.</td>
</tr>
<tr>
<td>Dansk [Danish]</td>
<td>Undertegnede NETGEAR Inc. erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.</td>
</tr>
<tr>
<td>English</td>
<td>Hereby, NETGEAR Inc., declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.</td>
</tr>
<tr>
<td>Español [Spanish]</td>
<td>Por medio de la presente NETGEAR Inc. declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.</td>
</tr>
<tr>
<td>Ελληνική [Greek]</td>
<td>ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ NETGEAR Inc. ΔΗΛΩΝΕΙ ΟΤΙ Ραδιολαν ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.</td>
</tr>
<tr>
<td>Français [French]</td>
<td>Par la présente NETGEAR Inc. déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.</td>
</tr>
<tr>
<td>Italiano [Italian]</td>
<td>Con la presente NETGEAR Inc. dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.</td>
</tr>
<tr>
<td>Nederlandse [Dutch]</td>
<td>Hierbij verklaart NETGEAR Inc. dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.</td>
</tr>
</tbody>
</table>
FCC Requirements for Operation in the United States

FCC Information to User
This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration Of Conformity
We, NETGEAR, Inc., 350 East Plumeria Drive, Santa Clara, CA 95134, declare under our sole responsibility that the NETGEAR® GS108T and GS110TP Smart Switches complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:
• This device may not cause harmful interference, and
• This device must accept any interference received, including interference that may cause undesired operation.

EODC in Languages of the European Community

<table>
<thead>
<tr>
<th>Language</th>
<th>Translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magyar [Hungarian]</td>
<td>Alulirott, NETGEAR Inc. nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.</td>
</tr>
<tr>
<td>Polski [Polish]</td>
<td>Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.</td>
</tr>
<tr>
<td>Português [Portuguese]</td>
<td>NETGEAR Inc. declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.</td>
</tr>
<tr>
<td>Slovensko [Slovenian]</td>
<td>NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.</td>
</tr>
<tr>
<td>Slovensky [Slovak]</td>
<td>NETGEAR Inc. týmto vyhlasuje, že Radiolan splňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.</td>
</tr>
<tr>
<td>Svenska [Swedish]</td>
<td>Härmed intygar NETGEAR Inc. att denna Radiolan står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.</td>
</tr>
<tr>
<td>Íslenska [Icelandic]</td>
<td>Hér með lífsir NETGEAR Inc. yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.</td>
</tr>
<tr>
<td>Norsk [Norwegian]</td>
<td>NETGEAR Inc. erklærer herved at utstyret Radiolan er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.</td>
</tr>
</tbody>
</table>
FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus, (NETGEAR® GS108T and GS110TP Smart Switches), does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Canada ID: 4054A-FVX538
Numerics
802.1X  147, 164
   example configuration 254

A
access control
   ACL example configuration 246
   ACLs 180
   management interface 157
authentication
   802.1X 164, 254
   enable 29
   list 155
   port-based 164
   RADIUS 147, 149
   SNMP 29, 57, 58
   TACACS+ 153
Auto-Video 84, 108

C
certificate 159
changing the password 18, 146
Configuration
   802.1X 164
   Access Control Lists 180
   Access Profile 161
   Access Rule 162
   Authentication List 155
   Class 135
   Community 54
   CoS 126
   DHCP Filtering 72
   Differentiated Services 133
   Diffserv 134
   DNS 44
   Dual Image 228
   Dynamic Address 123
   Dynamic Host 46
   Global 109
   Green Ethernet 47
   HTTP 157
   IGMP Snooping 109
   LACP 82
   LACP Port 83
   LAG 79
   LLDP 59
   MAC Filter 171
   Management Access 157
   MST Port 104
   Network Settings on the Administrative System 15
   password 146
   Policy 138
   Port Security 175
   Port VLAN ID 87
   RADIUS 147
      Global 147
   Secure HTTP 158
   SNMP v3 User 58
   SNTP Server 39
   Standard IP ACL Example 248
   STP 94
   TACACS+ 153
   Time 37
   Trap 55
   VLAN 84
   VLAN example 245
   VLAN Port Membership 86
   CoS 126

D
defaults 238
   CoS 247
      factory 147
   DES 29
   Device View 26
   DHCP
      client 11
      Filtering 72
      Filtering Interface Configuration 73
      refreshing the client 18
   DiffServ 133
   DNS 44
   DoS 42
   download
      a file 224
      files via HTTP 223
      from a remote system 223
      software 223
   Dual Image Status 229
E
EAP 206
EAPOL 207

F
file management 228
firmware 21
firmware download 223

G
Green Ethernet 47, 77
guest VLAN configuration 255

H
help, HTML-based 26
HTTP 157
  management interface access 17
  secure 157
  using to download files 225
HTTPS 158

I
ICMP 42
IEEE 802.11x 254
IEEE 802.1AB 59
IEEE 802.1D 94
IEEE 802.1Q 84, 94
IEEE 802.1s 94
IEEE 802.1w 94
IEEE 802.1X 147
IEEE 802.3 flow control 78
IGMP 109
  snooping 109
  snooping querier 117
interface
  LAG 79
  logical 30
  naming convention 30
  physical 30
  queue configuration 129
IP address
  administrative system 15
  switch 11, 34
IP DSCP 126
  Mapping 131

L
LACP port configuration 83
LAG VLAN 79
LAGPDUs 79
LAGs 79
  Membership 81
  Static 79
LLDP 59
  Local Information 65
  neighbors information 67
  packets 60
  port settings 61
LLDP-MED 59

M
MAC 34, 66, 100, 109
  ACL 182
  bridge identifier 103
  CPU Management Interface 30
  dynamic address 123
  filter summary 173
  MFDB Table 114
  multicast destination 113
  rules 183
  searching address table 121
  Static Address 124
MD5 37
MIBs 29
multicast, layer 2 109

N
navigation 25

O
OUI 91

P
password
  change 18, 146
  login 146
Ping 231
PoE 12, 14, 48
port
  authentication 164
  summary 169
Power Sourcing Equipment. See PSE
PSE 12, 14
Q
QoS 125
  802.1p to Queue Mapping 130

R
RADIUS 146
  server 147
  statistics 149
reboot 18, 220
reset
  button 147
  configuration to defaults 221
  switch 220
RSTP 94

S
Security MAC Address 178
server, HTTP 157
severity, log message 211
Simple Network Time Protocol 36
SNMP
  traps 55
  using 29
  v1, v2 54
  v3 58
SNTP 36
  Global Status 38
  global status 38
  server configuration 39
  server status 41
specifications 238
SSL 158
storm control 174
STP 94
  example configuration 257
  Status 95
Stratum
  0 36
  1 36
  2 36

T
T1 37
T2 37
T3 37
T4 37
TACACS+
  folder 153
  settings 153
  technical support 2
Time
  configure through SNTP 38
  UTC 38
  time 36
    clock source 38
    levels 36
    local 38
    zone 38
TraceRoute 232
trademarks 2
traffic control 171
trap
  flags 57
  manager 57

U
Unicast 37
upload configuration 222

V
video 84
VLAN 84
  example configuration 244
  guest 165, 167, 254
  ID 84
  management 35
  managing 84
  Port VLAN ID 87
  PVID 87
  voice 89
Voice VLAN OUI 91
VoIP 91, 93

W
Web interface panel 24