S350 Series 24-Port (PoE+) and 48-Port Gigabit Ethernet Smart Managed Pro Switches with 2 or 4 SFP Ports

Models
GS324T
GS324TP
GS348T
Support
Thank you for purchasing this NETGEAR product. You can visit https://www.netgear.com/support/ to register your product, get help, access the latest downloads and user manuals, and join our community. We recommend that you use only official NETGEAR support resources.

Compliance and Conformity
For regulatory compliance information including the EU Declaration of Conformity, visit https://www.netgear.com/about/regulatory/.
See the regulatory compliance document before connecting the power supply.
Do not use this device outdoors. If you connect cables or devices that are outdoors to this device, see http://kb.netgear.com/000057103 for safety and warranty information.

Trademarks
© NETGEAR, Inc., NETGEAR, and the NETGEAR Logo are trademarks of NETGEAR, Inc. Any non-NETGEAR trademarks are used for reference purposes only.

Revision History

<table>
<thead>
<tr>
<th>Publication Part Number</th>
<th>Publish Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>202-11890-02</td>
<td>April 2019</td>
<td>We made very minor changes and corrections.</td>
</tr>
<tr>
<td>202-11890-01</td>
<td>March 2019</td>
<td>First publication.</td>
</tr>
</tbody>
</table>
Contents

Chapter 1  Get Started

Available Publications .......................................................... 10
Switch Management and Discovery Overview ......................... 11
Options to Change the Default IP Address of the Switch .......... 11
Discover or Change the Switch IP Address ............................. 12
  Discover the Switch in a Network With a DHCP Server ........... 12
  Discover the Switch in a Network Without a DHCP Server ....... 13
  Use the NETGEAR Switch Discovery Tool to Access the Switch ... 15
  Use the NETGEAR Insight Mobile App to Discover the Switch ... 16
  Configure a Static IP Address From a Directly Connected Computer .. 16
About the User Interfaces ...................................................... 18
  Software Requirements to Use the Local Browser Interface ....... 18
Supported Web Browsers ...................................................... 18
Access the Local Browser Interface ....................................... 19
  Navigation Tabs, Configuration Menus, and Page Menu ......... 20
  Configuration and Status Options .................................... 21
  Buttons in the Local Browser Interface ............................. 21
  User-Defined Fields .................................................... 21
Change the Language of the Local Browser Interface ............... 22
Use the Device View of the Local Browser Interface ............... 22
  Power LED in the Device View ....................................... 24
  Fan LED in the Device View (Models GS324TP and GS348T) ...... 24
  PoE Max LED in the Device View (Model GS324TP) ................ 25
Interface Naming Conventions ............................................. 25
Configure Interface Settings .............................................. 25
Context-Sensitive Help and Access to the Support WebSite ......... 28
Access the User Guide Online ............................................. 29
Register Your Product ....................................................... 30

Chapter 2  Configure System Information

View and Configure the Switch Management Settings ............... 32
View or Define System Information ..................................... 32
View the System CPU Status ............................................. 37
Configure the IP Network and VLAN Settings for the Local Browser Interface .................................................. 40
Change the Management VLAN ......................................... 41
Configure the Time Settings ............................................. 42
Configure Denial of Service Settings .................................. 55
Configure DNS Settings .................................................. 58
Configure Green Ethernet Settings ........................................ 63
Use the Device View ............................................................ 72
Configure PoE ........................................................................ 72
Configure the Global PoE Settings .......................................... 72
Configure the PoE Port Settings .............................................. 74
Configure SNMP .................................................................... 77
Configure the SNMPv1/v2 Community .................................... 77
Configure SNMPv1/v2 Trap Settings ....................................... 80
Configure SNMPv1/v2 Trap Flags ........................................... 82
View the Supported MIBs ...................................................... 83
Configure SNMP V3 Users ..................................................... 84
Configure LLDP ...................................................................... 85
Configure LLDP Global Settings ............................................ 85
Configure LLDP Port Settings ................................................ 87
View the LLDP-MED Network Policy ....................................... 88
Configure LLDP-MED Port Settings ....................................... 90
View the LLDP-MED Neighbors Information ............................ 91
View the Local Information Advertised Through LLDP ............ 93
View LLDP Neighbors Information ........................................ 96
Configure DHCP Snooping .................................................... 99
Configure the Global DHCP Snooping Settings ...................... 99
Enable DHCP for All Interfaces in a VLAN ......................... 100
Configure DHCP Snooping Interface Settings ....................... 101
Configure Static DHCP Bindings .......................................... 103
Configure DHCP Snooping Persistent Settings ...................... 104
View or Clear DHCP Snooping Statistics .............................. 105
Set Up PoE Timer Schedules ............................................... 106
Create a PoE Timer Schedule ............................................... 106
Specify the Settings for an Absolute PoE Timer Schedule ......... 107
Specify the Settings for a Recurring PoE Timer Schedule ......... 108
Change the Settings for a Recurring PoE Timer Schedule Entry ... 110
Delete a PoE Timer Schedule Entry .................................... 111
Delete a PoE Timer Schedule ............................................... 111

Chapter 3 Configure Switching

Configure the Port Settings and Maximum Frame Size ........... 114
Configure Link Aggregation Groups ...................................... 117
Configure LAG Settings ....................................................... 117
Configure LAG Membership ............................................... 119
Set the LACP System Priority ............................................. 120
Set the LACP Port Priority Settings ..................................... 121
Configure VLANs ............................................................... 122
Configure VLAN Settings .................................................... 123
Configure VLAN Membership ............................................. 125
View the VLAN Status ....................................................... 127
Configure Port PVID Settings .............................................. 129
Configure a MAC-Based VLAN ........................................... 131
Configure Protocol-Based VLAN Groups ............................................. 133
Configure Protocol-Based VLAN Group Membership .......................... 134
Configure a Voice VLAN ..................................................................... 135
Configure Auto-VoIP ......................................................................... 137
Configure Protocol-Based Port Settings for VoIP ................................. 137
Configure Auto-VoIP OUI-Based Properties ....................................... 139
Configure the OUI-Based Port Settings ............................................. 140
Manage the OUI Table ....................................................................... 141
Display the Auto-VoIP Status .............................................................. 143
Configure Spanning Tree Protocol ..................................................... 143
Configure the STP Settings and View the STP Status ............................ 144
Configure and View the CST Settings ................................................. 146
Configure and View the CST Port Settings ........................................ 148
View the CST Port Status .................................................................. 150
View Rapid STP Information ............................................................... 152
Manage MST Settings ..................................................................... 153
Configure and View the Port Settings for an MST Instance .................. 155
View the STP Statistics ..................................................................... 158
Configure Multicast ......................................................................... 159
View, Search, or Clear the MFDB Table ............................................ 159
View the MFDB Statistics .................................................................. 160
Configure the Auto-Video Multicast Settings ...................................... 161
About IGMP Snooping ...................................................................... 162
Configure IGMP Snooping .................................................................. 163
Configure IGMP Snooping for Interfaces .......................................... 164
View, Search, or Clear the IGMP Snooping Table ................................. 166
Configure IGMP Snooping for VLANs .............................................. 167
Modify IGMP Snooping Settings for a VLAN ...................................... 168
Disable IGMP Snooping on a VLAN .................................................. 169
Configure a Multicast Router Interface ............................................ 169
Configure a Multicast Router VLAN ............................................... 171
IGMP Snooping Querier Overview ..................................................... 172
Configure an IGMP Snooping Querier .............................................. 172
Configure an IGMP Snooping Querier for VLANs ............................... 173
Display IGMP Snooping Querier for VLAN Status ............................ 174
View, Search, and Manage the MAC Address Table ......................... 175
View, Search, or Clear the MAC Address Table .................................. 176
Set the Dynamic Address Aging Interval .......................................... 177
Add a Static MAC Address to the MAC Address Table .................. 178
Configure Layer 2 Loop Protection .................................................. 179
Configure Global Layer 2 Loop Protection ......................................... 179
View and Configure Layer 2 Loop Protection on a Port ...................... 180

Chapter 4 Configure Quality of Service

Quality of Service Concepts ............................................................. 184
Manage Class of Service ................................................................. 184
CoS Configuration Concepts ............................................................ 184
Configure Global CoS Settings .......................................................... 185
Configure CoS Interface Settings for an Interface .................. 186
Configure CoS Queue Settings for an Interface .................. 188
Map 802.1p Priorities to Queues ................................. 190
Map DSCP Values to Queues ..................................... 191
Manage Differentiated Services ...................................... 192
Defining DiffServ .................................................. 193
Configure and Display Global DiffServ Settings .................. 193
Configure a DiffServ Class ........................................ 195
Configure a DiffServ Policy ....................................... 200
Configure the DiffServ Service Interface ......................... 205
View DiffServ Service Statistics .................................... 207

Chapter 5  Manage Device Security

Configure the Management Security Settings ...................... 210
Change the Password for the Local Browser Interface .......... 210
Manage the RADIUS Settings ...................................... 211
Configure TACACS+ ................................................ 219
Configure Authentication Lists ..................................... 223
Manage the Smart Control Center Utility ......................... 227
Configure Management Access ..................................... 227
Configure HTTP Access Settings .................................. 228
Configure HTTPS Access Settings ................................. 229
Manage Certificates for HTTPS Access ............................ 230
Transfer an Existing Certificate to the Switch ................... 232
Manage Access Control to the Switch .............................. 234
Configure Port Authentication ...................................... 240
Configure Global 802.1X Settings ................................ 240
Manage Port Authentication on Individual Ports ................. 242
View the Port Summary ............................................. 246
View the Client Summary .......................................... 247
Set Up Traffic Control .............................................. 249
Manage MAC Filtering ................................................. 249
MAC Filter Summary ................................................. 251
Configure Storm Control Settings ................................ 252
Manage Port Security ................................................. 256
Configure Protected Ports .......................................... 260
Configure Access Control Lists ..................................... 261
Use the ACL Wizard to Create a Simple ACL ..................... 261
Configure a Basic MAC ACL ....................................... 266
Configure MAC ACL Rules ......................................... 268
Configure MAC Bindings ............................................. 272
View or Delete MAC ACL Bindings in the MAC Binding Table . 274
Configure a Basic or Extended IP ACL ............................ 275
Configure Rules for a Basic IP ACL ............................... 278
Configure Rules for an Extended IP ACL ......................... 282
Configure IP ACL Interface Bindings .............................. 289
View or Delete IP ACL Bindings in the IP ACL Binding Table .... 291
Chapter 6  Monitor the System

Monitor the Switch and the Ports ........................................... 294
View Switch Statistics ..................................................... 294
View Port Statistics .......................................................... 297
View and Manage Detailed Port Statistics .............................. 300
View or Clear EAP and EAPoL Statistics ............................... 306
Perform a Cable Test (Model GS348T) .................................. 308
Configure and View Logs .................................................... 309
Manage the Memory Logs ................................................... 309
Manage the Flash Log ......................................................... 311
Manage the Server Log ....................................................... 313
View or Clear the Trap Logs and Counters ............................ 316
View or Clear the Event Log ................................................. 317
Configure Port Mirroring .................................................... 319

Chapter 7  Maintenance

Reboot the Switch ............................................................. 323
Reset the Switch to Its Factory Default Settings ..................... 324
Export a File From the Switch .............................................. 325
Use TFTP to Export a File From the Switch to a TFTP Server .... 325
Use HTTP to Export a File from the Switch to a Computer ...... 326
Download a File to the Switch or Update the Firmware ............ 327
Use TFTP to Download a File to the Switch or Update the Software Image ......................................................... 328
Use HTTP to Download a File to the Switch or Update the Software Image ......................................................... 330
Manage Software Images ................................................... 332
Copy a Software Image ....................................................... 332
Configure Dual Image Settings ............................................. 333
View the Dual Image Status ................................................... 335
Enable Remote Diagnostics .................................................. 336

Appendix A  Configuration Examples

Virtual Local Area Networks (VLANs) ...................................... 338
VLAN Configuration Examples ............................................. 339
Access Control Lists (ACLs) .................................................. 340
MAC ACL Sample Configuration ............................................ 340
Standard IP ACL Sample Configuration ............................... 341
Differentiated Services (DiffServ) ........................................... 342
Class ................................................................. 343
DiffServ Traffic Classes ....................................................... 344
Creating Policies ............................................................. 344
DiffServ Example Configuration .......................................... 345
802.1X Access Control ....................................................... 346
802.1X Example Configuration ............................................ 348
Multiple Spanning Tree Protocol ............................................ 349
Get Started

This user manual describes how you can configure and operate the NETGEAR S350 Series 24-Port (PoE+) and 48-Port Gigabit Ethernet Smart Managed Pro Switches with 2 or 4 SFP Ports by using the local browser–based management interface.

The manual describes the software configuration procedures and explains the options that are available within those procedures for the following models:

- **GS324T**: S350 Series 24-Port Gigabit Ethernet Smart Managed Pro Switch with 2 SFP Ports
- **GS324TP**: S350 Series 8-Port Gigabit PoE+ Ethernet Smart Managed Pro Switch with 2 SFP Ports
- **GS348T**: S350 Series 48-Port Gigabit Ethernet Smart Managed Pro Switch with 4 SFP Ports

This chapter provides an overview of how you can start your switch and access the local browser–based management interface.

The chapter contains the following sections:

- Available Publications
- Switch Management and Discovery Overview
- Options to Change the Default IP Address of the Switch
- Discover or Change the Switch IP Address
- About the User Interfaces
- Access the Local Browser Interface
- Navigation Tabs, Configuration Menus, and Page Menu
- Change the Language of the Local Browser Interface
- Use the Device View of the Local Browser Interface
- Interface Naming Conventions
- Configure Interface Settings
- Context-Sensitive Help and Access to the Support WebSite
- Access the User Guide Online
- Register Your Product
Note: In this manual, the local browser–based management interface is referred to as the local browser interface.

Note: For more information about the topics covered in this manual, visit the support website at netgear.com/support.

Note: Firmware updates with new features and bug fixes are made available from time to time at netgear.com/support/download/. Some products can regularly check the site and download new firmware, or you can check for and download new firmware manually. If the features or behavior of your product does not match what is described in this guide, you might need to update your firmware.

Available Publications

The following guides are available at netgear.com/support/download/:

- Installation Guide
- Hardware Installation Guide
Switch Management and Discovery

Overview

The switch provides administrative management options that let you configure, monitor, and control the network. Using the local browser interface, you can configure the switch and the network, including the ports, the management VLAN, VLANs for traffic control, link aggregation for increased bandwidth, quality of service (QoS) for prioritizing traffic, and network security.

Initial discovery of the switch on the network requires one of the following tools:

- **NETGEAR Smart Control Center (SCC) program.** The SCC runs on a Windows-based computer. You can download the SCC program from netgear.com/support/download/. For more information about the SCC program see Discover the Switch in a Network With a DHCP Server on page 12 and Discover the Switch in a Network Without a DHCP Server on page 13.

- **NETGEAR Switch Discovery Tool.** If you use a Mac computer, you can use the NETGEAR Switch Discovery Tool to discover the switch in your network and access the local browser interface of the switch. For more information about the Switch Discovery Tool, Use the NETGEAR Switch Discovery Tool to Access the Switch on page 15.

- **NETGEAR Insight mobile app.** You can also install the NETGEAR Insight mobile app on an iOS or Android mobile device and discover the IP address of the switch. For more information about the Insight mobile app, see Use the NETGEAR Insight Mobile App to Discover the Switch on page 16.

You can also get the IP address of the switch from the DHCP server in the network or use an IP scanner utility.

After discovery, you can configure the switch using the local browser interface for advanced setup and configuration of features, or the SCC program for very basic setup. For more information, see the SCC user manual, which you can download from netgear.com/support/download/.

Options to Change the Default IP Address of the Switch

To enable remote management of the switch through a web browser or SNMP, connect the switch to the network and specify an IP address, subnet mask, and default gateway. The switch default IP address is 192.168.0.239 and the default subnet mask is 255.255.255.0.
To change the default IP address of the switch, use one of the following methods:

- **Dynamic assignment through DHCP.** DHCP is enabled on the switch by default. 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 Discover the Switch 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 include 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 Discover the Switch in a Network Without a DHCP Server on page 13.

- **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 computer in the 192.168.0.0/24 network and change the settings by using the local browser interface on the switch. For information about how to set the IP address on the computer so that it is in the same subnet as the default IP address of the switch, see Configure a Static IP Address From a Directly Connected Computer on page 16.

## Discover or Change the Switch IP Address

The following sections describe methods that let you discover or change the IP address of the switch.

### Discover the Switch in a Network With a DHCP Server

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

**Note:** For more information about the SCC program, see the SCC user manual, which you can download by visiting netgear.com/support/download/.

**To install the switch in a network with a DHCP server:**

1. Connect the switch to a network with a DHCP server.
2. Power on the switch by connecting its power cord.
3. Install the Smart Control Center on your computer.
4. Start the Smart Control Center.
5. Click the Discover button for the Smart Control Center to discover all the devices in the subnet.
6. Make a note of the displayed IP address assigned by the DHCP server. You can use IP address later to access the switch directly from a web browser (that is, without using the Smart Control Center).

7. Select your switch by clicking the line that displays the switch.

8. Click the **Web Browser Access** button. The Smart Control Center launches a browser that displays the login page of the selected device.

Use your web browser to manage your switch. The default password is **password**. For more information about the page layout and options, see Navigation Tabs, Configuration Menus, and Page Menu on page 20.

**Discover the Switch in a Network Without a DHCP Server**

This section describes how to use the Smart Control Center (SCC) to set up your switch in a network without a DHCP server. If your network does not include a DHCP service, you must assign a static IP address to your switch.

If you prefer, you can assign the switch a static IP address even if your network does include a DHCP server.

**Note:** For more information about the SCC program, see the SCC user manual, which you can download by visiting netgear.com/support/download/.
To assign a static IP address:
1. Connect the switch to your existing network.
2. Power on the switch by connecting its power cord.
3. Install the Smart Control Center on your computer.
4. Start the Smart Control Center.
5. Click the Discover button for the Smart Control Center to find your switch.
   The utility broadcasts Layer 2 discovery packets within the broadcast domain to discover the switch.
6. Select the switch, and then click the Configure Device button.
   The page expands to display additional fields at the bottom.
7. Select the Disabled radio button.
   DHCP is disabled.
8. Enter the static switch IP address, gateway IP address, and subnet mask for the switch.
9. Type your password to continue with the configuration change.
   Tip: You must enter the current password each time that you use the Smart Control Center to update the switch settings. The default password is password.
10. Click the Apply button.
    Your settings are saved.
Use the NETGEAR Switch Discovery Tool to Access the Switch

For easiest access, we recommend that you cable the switch to a network with a router or DHCP server that assigns IP addresses, power on the switch, and then use a computer that is connected to the same network as the switch.

The NETGEAR Switch Discovery Tool lets you discover the switch in your network and access the local browser interface of the switch from a Mac or a 64-bit Windows-based computer.

To install the NETGEAR Switch Discovery Tool, discover the switch in your network, and access the local browser interface of the switch:

1. Download the Switch Discovery Tool by visiting netgear.com/support/product/netgear-switch-discovery-tool.aspx. Depending on the computer that you are using, download either the Mac version or the version for a 64-bit Windows-based computer.

2. Temporarily disable the firewall, Internet security, antivirus programs, or all of these on the computer that you use to configure the switch.

3. Unzip the Switch Discovery Tool files, double-click the .exe or .dmg file (for example, NETGEAR+Switch+Discovery+Tool+Setup+1.2.101.exe or NetgearSDT-V1.2.101.dmg), and install the program on your computer. The installation process places a NETGEAR Switch Discovery Tool icon on your desktop.

4. Reenable the security services on your computer.

5. Power on the switch. The DHCP server assigns the switch an IP address.

6. Connect your computer to the same network as the switch. You can use a WiFi or wired connection. The computer and the switch must be on the same Layer 2 network.

7. Open the Switch Discovery Tool. To open the program, double-click the NETGEAR Switch Discovery Tool icon on your desktop. The initial page displays a menu and a button.

8. From the Choose a connection menu, select the network connection that allows the Switch Discovery Tool to access the switch.

9. Click the Start Searching button. The Switch Discovery Tool displays a list of Smart Managed Plus Switches that it discovers on the selected network. For each switch, the tool displays the IP address.
10. To access the local browser interface of the switch, click the ADMIN PAGE button. The login page of the local browser interface opens.

11. Enter the switch password. The default password is password. The password is case-sensitive. The Switch Information page displays.

Use the NETGEAR Insight Mobile App to Discover the Switch

If the switch is connected to a WiFi router or access point, the NETGEAR Insight mobile app lets you discover the switch in your network.

To use the NETGEAR Insight mobile app to discover the switch in your network:

1. On your iOS or Android mobile device, go to the app store, search for NETGEAR Insight, and download and install the app.
2. Connect your mobile device to the WiFi network of the WiFi router or access point to which the switch is connected.
3. Open the NETGEAR Insight mobile app.
4. Select LOG IN to log in to your existing NETGEAR account or tap the CREATE NETGEAR ACCOUNT button to create a new account.

After you log in to your account, the IP address of the switch displays in the device list.

5. Write down the IP address for future use.

Configure a Static IP Address From a Directly Connected Computer

If you do not want to use the Smart Control Center to configure the network information on the switch, you can change the IP address of the switch by connecting an Ethernet cable from a computer to the switch. The IP address of the computer must be in the same subnet as the default IP address on the switch. For most networks, this means that you must change the IP address of the computer to be on the same subnet as the default IP address of the switch (192.168.0.239).

To configure a static IP address on the switch:

1. Change the IP settings of your computer to be in the same subnet as the IP settings of the switch.

If the DHCP client of the switch is enabled and you remove the switch from the network with the DHCP server, the IP address reverts to the default IP address of 192.168.0.239 with a subnet of 255.255.255.0.
**Note:** If you already disabled the DHCP client and assigned a static IP address to the switch, change the IP settings of your computer to be in the same subnet as the static IP address.

For more information about changing the IP settings on your computer, see one of the following knowledge base articles at the NETGEAR website:

- **Windows-based computer.** See the following article: https://kb.netgear.com/27476/How-to-set-a-static-IP-address-in-Windows
- **Mac.** See the following article: https://kb.netgear.com/000037250/Set-ting-a-static-IP-address-on-your-network-a-dapter-in-Mac-OS-for-direct-access-to-an-access-point

(The Mac article is written for an access point but is also valid for a switch.)

2. Connect your computer to the switch using an Ethernet cable.
3. Power on the switch by connecting its power cord.
4. Launch a web browser.
5. In the address field of your web browser, enter the IP address of the switch.
   - If you did not disable the DHCP client and assigned a static IP address to the switch, enter **192.168.0.239**.
   - The login window opens.
6. Enter the switch’s password in the **Password** field.
   - The default password is **password**.
   - The System Information page displays.
7. **Select System > Management > IP Configuration.**
   - The IP Configuration page displays.
8. Select the **Static IP Address** radio button.
9. Configure the IP address, subnet mask, and default gateway to be assigned to the switch.
10. Click the **Apply** button.
    - Your settings are saved.

Disconnect the Ethernet cable and return the network configuration on your computer to the original settings.
About 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:

- Local browser interface (which used to be referred to as the web 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.

This manual describes how to use the local browser interface to manage and monitor the system.

Software Requirements to Use the Local Browser 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

Supported Web Browsers

The following browsers were tested and support the local browser interface. Later browser versions might function fine but were not tested. The supported web browsers include the following:

- Microsoft Internet Explorer (IE) version 11
- Microsoft Edge
- Mozilla Firefox versions 64
- Chrome version 62
- Safari on MAC OS X version 11.0
Access the Local Browser Interface

You must be able to ping the IP address of the switch from your computer 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 in the address field.

You can use one of the following methods to access the switch local browser interface:

- From the Smart Control Center, select the switch and click the **Web Browser Access** button.
- From the Switch Discovery Tool, select the switch and click the **ADMIN PAGE** button.
- Open a web browser and enter the IP address of the switch in the address field.

If you use any of these methods, the switch Login window displays.

To access the switch local browser interface from a web browser:

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.
   - The login window opens.
4. If the browser does not display the login window, do the following:
   - If you use a wired Ethernet connection, make sure that the computer is connected to the same network that the switch is attached to or directly to one of the LAN Ethernet ports of the switch.
   - If you use a mobile device, make sure that mobile device is connected to an access point that is attached to the same network that the switch is connected to or that the access point is directly attached to one of the LAN Ethernet ports of the switch.
   - Make sure that the switch is receiving power and that its Power LED is lit.
   - Close and reopen the browser.
5. Enter the switch’s password in the **Password** field.
   - The default password is **password**.
   - The System Information page displays.
   - The following figure shows the layout of the local browser interface.
Navigation Tabs, Configuration Menus, and Page Menu

The navigation tabs along the top of the local browser 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 menus directly under the tabs. The configuration menus in the blue bar change according to the navigation tab that is selected.

The configuration pages for each feature are available as submenu links in the page menu on the left side of the page. Some items in the menu expand to reveal multiple submenu links, as the following figure shows.
Configuration and Status Options

The area directly under the configuration menus and to the right of the links displays the configuration information or status for the page you select. On pages that contain configuration options, you might be able to enter information into fields, select options from menus, select check boxes, and select radio buttons.

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

Buttons in the Local Browser Interface

Each page also contains command buttons. The following table shows the command buttons that are used throughout the pages in the local browser interface:

Table 1. Command buttons in the local browser interface

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

User-Defined Fields

User-defined fields can contain 1 to 159 characters, unless otherwise noted on the configuration web page. All characters can be used except for the ones stated in the following table (unless specifically noted in a procedure for a feature).

Table 2. Invalid characters for user-defined fields

<table>
<thead>
<tr>
<th>Invalid Characters for user-defined fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>\ &lt;</td>
</tr>
<tr>
<td>/ &gt;</td>
</tr>
<tr>
<td>&quot; &quot;</td>
</tr>
<tr>
<td>?</td>
</tr>
</tbody>
</table>
Change the Language of the Local Browser Interface

By default, the language is set to Auto. You can set the language to a specific one.

**To change the language of the local browser interface:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.
   
   The System Information page displays.

5. At the top of the page, to the left of **Welcome**, select a language from the language menu.
   
   A confirmation pop-up window opens.

6. Click the **OK** button to confirm.
   
   The switch restarts and you must log in again.
   
   The language of the local browser interface is now set to the language that you selected.

Use the Device View of the Local Browser Interface

The Device View displays the ports on the switch. This graphic tool provides an alternate way to navigate to configuration and monitoring options. The graphic tool also provides information about device ports, configuration and status, tables, and feature components.
To use Device View:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select System > Device View.
   The Device View page displays.
   The following figure shows the Device View page for model GS324TP.

![Device View Page](image)

Depending upon the link status of the port, both the port and the associated port LED display green, yellow, or black:

- **Green.** The port is linking at a speed of 1 Gbps.
- **Yellow.** The port is linking at a speed of 10 Mbps or 100 Mbps.
- **Black or gray.** No link is present.

For models GS324T and GS324TP, the associated port LED is at the upper left of the panel. For model GS348T, the associated port LED is above the port.

For model GS324TP, depending on the PoE status of the port, the associated PoE LED at the lower left of the panel is either green, yellow, or black:

- **Green.** The port is delivering PoE power.
- **Yellow.** A PoE fault occurred.
- **Black or gray.** The port is not delivering PoE power.

6. Click a port to open a menu that displays statistics and configuration options.
   You can select a menu option to access the page that contains the configuration or monitoring options.
If you right-click the graphic, but do not right-click a specific port, the main menu displays. This menu contains the same options as the navigation tabs at the top of the page.

The following figure shows the details on the Device View page for model GS324TP.

Right-click the specific port that you want to view or configure to see a menu that displays statistics and configuration options. Select the menu option to access the page that contains the configuration or monitoring options.

The system LEDs are located on the left side of the front panel.

### Power LED in the Device View

The Power LED is a bicolor LED that serves as an indicator of the power and diagnostic status:

- **Solid green.** The switch is powered on and operating normally.
- **Solid yellow.** The switch is booting.
- **Off.** Power is not supplied to the switch.

### Fan LED in the Device View (Models GS324TP and GS348T)

The Fan LED serves as an indicator of the fan and diagnostic status:

- **Off.** The fan is operating normally.
- **Solid yellow.** A problem occurred with the fan.

---

**Note:** Model GS324T does not include a fan.
PoE Max LED in the Device View (Model GS324TP)

The PoE Max LED indicates the following status:

- **Off.** Sufficient (more than 7W of) PoE power is available.
- **Solid yellow.** Less than 7W of PoE power is available.
- **Blinking yellow.** At least once during the previous two minutes, less than 7W of PoE power was available.

Interface Naming Conventions

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 1.</td>
<td>g1, g2, g12</td>
</tr>
<tr>
<td>Link aggregation group (LAG)</td>
<td>LAG interfaces are logical interfaces that are used only for bridging functions.</td>
<td>l1, l2, l3</td>
</tr>
<tr>
<td>CPU management interface</td>
<td>This is the internal switch interface that is associated with the switch base MAC address. The interface is not configurable and is always listed in the MAC Address Table.</td>
<td>c1</td>
</tr>
</tbody>
</table>

Configure Interface Settings

For some features that allow you to configure interface settings, you can apply the same settings simultaneously to any of the following:

- A single port
- Multiple ports
- All ports
- A single LAG
- Multiple LAGs
- All LAGs
- Multiple ports and LAGs
- All ports and LAGs
Many of the pages that allow you to configure or view interface settings include links to display all ports, all LAGs, or all ports and LAGs on the page.

Use these links as follows:

- To display all ports, click the 1 link.
- To display all LAGs, click the LAG link.
- To display all ports and LAGs, click the All link.

The procedures in this section describe how to select the ports and LAGs to configure. The procedures assume that you are already logged in to the switch. If you do not know how to log in to the switch, see Navigation Tabs, Configuration Menus, and Page Menu on page 20.

To configure a single port by using the Go To Interface field:
1. Ensure that the page is displaying all ports, and not only the LAGs.
2. In the Go To Interface field, type the port number.
   For example, type g4.
   For more information, see Interface Naming Conventions on page 25.
3. Click the Go button.
   The check box associated with the interface is selected, the row for the selected interface is highlighted, and the interface number displays in the heading row.
4. Configure the desired settings.
5. Click the Apply button.
   Your settings are saved.

To configure a single LAG by using the Go To Interface field:
1. Click the LAG link or the All link to display the LAGs.
2. In the Go To Interface field, type the LAG number, for example l3.
   For information, see Interface Naming Conventions on page 25.
3. Click the Go button.
   The check box associated with the interface is selected, the row for the selected interface is highlighted, and the interface number appears in the heading row.
4. Configure the desired settings.
5. Click the Apply button.
   Your settings are saved.

To configure a single port:
1. Ensure that the page is displaying all ports, and not only the LAGs.
2. Select the check box next to the port number.
The row for the selected interface is highlighted, and the interface number appears in the heading row.

3. Configure the desired settings.
4. Click the **Apply** button.
   
   Your settings are saved.

**To configure a single LAG:**

1. Click the **LAG** link or the **All** link to display the LAGs.
2. Select the check box next to the LAG number.
   
   The row for the selected interface is highlighted, and the interface number appears in the heading row.

3. Configure the desired settings.
4. Click the **Apply** button.
   
   Your settings are saved.

**To configure multiple ports:**

1. Ensure that the page is displaying all ports, and not only the LAGs.
2. Select the check box next to each port to configure.
   
   The row for each selected interface is highlighted.

3. Configure the desired settings.
4. Click the **Apply** button.
   
   Your settings are saved.

**To configure multiple LAGs:**

1. Click the **LAG** link or the **All** link to display the LAGs.
2. Select the check box next to each LAG to configure.
   
   The check box associated with each interface is selected, and the row for each selected interface is highlighted.

3. Configure the desired settings.
4. Click the **Apply** button.
   
   Your settings are saved.

**To configure all ports:**

1. Ensure that the page is displaying only ports, and not LAGs.
2. Select the check box in the heading row.
   
   The check boxes for all ports are selected and the rows for all ports are highlighted.

3. Configure the desired settings.
4. Click the **Apply** button.  
   Your settings are saved.  

**To configure all LAGs:**  
1. Click the **LAG** link to display only the LAG interfaces.  
2. Select the check box in the heading row.  
   The check box associated with every LAG is selected, and the rows for all LAGs are highlighted.  
3. Configure the desired settings.  
4. Click the **Apply** button.  
   Your settings are saved.  

**To configure multiple ports and LAGs:**  
1. Click the **All** link to display all ports and LAGs.  
2. Select the check box associated with each port and LAG to configure.  
   The rows for the selected ports and LAGs are highlighted.  
3. Configure the desired settings.  
4. Click the **Apply** button.  
   Your settings are saved.  

**To configure all ports and LAGs:**  
1. Click the **All** link to display all ports and LAGs.  
2. Select the check box in the heading row.  
   The check box associated with every port and LAG is selected, and the rows for all ports and LAGs are highlighted.  
3. Configure the desired settings.  
4. Click the **Apply** button.  
   Your settings are saved.  

**Context-Sensitive Help and Access to the Support WebSite**  

When you log in to the switch, every page contains a link to the online help (🔗) that 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 the link to the online help.
From the local browser interface, you can access the NETGEAR support website at netgear.com/support.

**To access the support website from the local browser interface:**
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address on page 12](#).
   The login window opens.
4. Enter the switch’s password in the **Password** field.
   The default password is `password`.
   The System Information page displays.
5. Select **Help > Support**.
   The Support page displays.
6. To access the NETGEAR support site for the switch, click the **Apply** button.

### Access the User Guide Online

The user manual (the guide you are now reading) is available at the NETGEAR download center at netgear.com/support/download/.

**To access the user manual online from the local browser interface:**
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address on page 12](#).
   The login window opens.
4. Enter the switch’s password in the **Password** field.
   The default password is `password`.
   The System Information page displays.
5. Select Help > Online Help > User Guide.
   The User Guide page displays.

6. To access the NETGEAR download center, click the **Apply** button.

7. Enter the model number of the switch.

8. Locate the user manual on the product support web page.

Register Your Product

To qualify for product updates and product warranty, we encourage you to register your product. The first time you log in to the switch, you can register with NETGEAR. Registration confirms that your email alerts work, lowers technical support resolution time, and ensures that your shipping address accuracy. We would also like to incorporate your feedback into future product development. We never sell or rent your email address and you can opt out of communications at any time.

To register with NETGEAR when you are prompted, click the **REGISTER NOW** button. Or at any time you can visit the NETGEAR website for registration at https://my.netgear.com/registration/login.aspx.

You can also use the NETGEAR Insight mobile app to register your product (see Use the NETGEAR Insight Mobile App to Discover the Switch on page 16).
2

Configure System Information

This chapter contains the following sections:

• View and Configure the Switch Management Settings
• Use the Device View
• Configure PoE
• Configure SNMP
• Configure LLDP
• Configure DHCP Snooping
• Set Up PoE Timer Schedules
View and Configure the Switch Management Settings

This section describes how to display the switch status and specify some basic switch information, such as the local browser interface IP address, system clock settings, and DNS information. The following sections describe how you can configure the switch management settings:

- View or Define System Information on page 32
- View the System CPU Status on page 37
- Configure the IP Network and VLAN Settings for the Local Browser Interface on page 40
- Configure the Time Settings on page 42
- Configure Denial of Service Settings on page 55
- Configure DNS Settings on page 58
- Configure Green Ethernet Settings on page 63

View or Define System Information

When you log in, the System Information page displays. You can configure and view general device information.

To view or define system information:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch's password in the Password field.
   The default password is password.
5. Define the following fields:
   - **System Name**: Enter the name to identify this switch. You can use up to 255 alphanumeric characters. The default is blank.
   - **System Location**: Enter the location of this switch. You can use up to 255 alphanumeric characters. The default is blank.
   - **System Contact**: Enter the contact person for this switch. You can use up to 255 alphanumeric characters. The default is blank.

6. Click the **Apply** button.

   Your settings are saved.

The following table describes the status information that displays in the System Information section.

**Table 4. System Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Name</td>
<td>The product name of this switch.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number of the switch.</td>
</tr>
<tr>
<td>System Object OID</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>The time in days, hours, and minutes since the last switch reboot.</td>
</tr>
<tr>
<td>Base Mac Address</td>
<td>Universally assigned hardware address of the switch.</td>
</tr>
<tr>
<td>Temp(C)</td>
<td>The general temperature of the switch in degrees Centigrade.</td>
</tr>
<tr>
<td>Temperature traps range</td>
<td>The minimum and maximum traps range.</td>
</tr>
</tbody>
</table>
View the Temperature Sensor Information

**Note:** The temperature sensor information is available for models GS324TP and GS348T.

You can view the current temperature of the temperature sensors. The maximum temperature of the temperature sensors depends on the hardware.

**To view temperature information:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
5. Scroll down to the Temperature Sensors section.
6. To refresh the page with the latest information about the switch, click the Refresh button.

The following table describes the status information that displays in the Temperature Sensors section.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor</td>
<td>The temperature sensor for the switch.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the temperature sensor.</td>
</tr>
<tr>
<td>Temp(C)</td>
<td>The temperature of the switch in degrees Centigrade.</td>
</tr>
<tr>
<td>State</td>
<td>The temperature state of the switch</td>
</tr>
<tr>
<td>Max Temp (C)</td>
<td>The maximum temperature of the CPU and MAC components. The switch shuts down if it exceeds the maximum temperature.</td>
</tr>
</tbody>
</table>
View the Fan Status

Note: The fan status information is available for models GS324TP and GS348T. Model GS324T does not include a fan.

You can view the status of the fans in all units. These fans remove the heat generated by the power, CPU, and other components, and allow the switch to function normally.

To view the fan status:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.

5. Scroll down to the Fans section.

6. To refresh the page with the latest information about the switch, click the Refresh button.

The following table describes the status information that displays in the Fans section.

### Table 6. Fans information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAN</td>
<td>The fan identifier.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the fan.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies whether the fan is fixed or removable.</td>
</tr>
<tr>
<td>Speed</td>
<td>The speed of the fan.</td>
</tr>
<tr>
<td>Duty level(%)</td>
<td>The duty level of the fan.</td>
</tr>
<tr>
<td>State</td>
<td>Specifies whether the fan is operational.</td>
</tr>
</tbody>
</table>
View the Power Supplies
You can view the status of the power supplies.

**To view the power supplies status:**
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address on page 12](#).
   The login window opens.
4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
5. Scroll down to the Power supplies section.
6. To refresh the page with the latest information about the switch, click the **Refresh** button.

The following table describes the status information that displays in the Power Supplies section.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power supply</td>
<td>The power supply identifier.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the power supply.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies whether the power supply is fixed or removable.</td>
</tr>
<tr>
<td>State</td>
<td>Specifies the state of the power supply.</td>
</tr>
</tbody>
</table>

View the Software Versions
You can view the software versions that are running on the switch.

**To view the software versions:**
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
5. Scroll down to the Versions section.

   To refresh the page with the latest information about the switch, click the Refresh button.

   Table 8. Versions information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Name</td>
<td>The model name of the switch.</td>
</tr>
<tr>
<td>Boot Version</td>
<td>The version of the bootloader software of the switch.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The version number of the software that is running on the switch.</td>
</tr>
</tbody>
</table>

View the System CPU Status

You can monitor the CPU, memory resources, and utilization patterns across various intervals to assess the performance, load, and stability settings of the switch.

To view the system CPU status:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
The default password is password.

The System Information page displays.

5. Select System > Management > System CPU Status > System CPU Status.

The CPU Utilization section shows the memory information, task-related information, and percentage of CPU utilization per task.

The following table describes CPU Memory Status information.

Table 9. CPU Memory Status information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total System Memory</td>
<td>The total memory of the switch in KBytes.</td>
</tr>
<tr>
<td>Available Memory</td>
<td>The available memory space for the switch in KBytes.</td>
</tr>
</tbody>
</table>

Configure the CPU Thresholds

The CPU Utilization Threshold notification feature allows you to configure thresholds that, when exceeded, trigger a notification. The notification occurs through SNMP trap and syslog messages.

To configure the CPU thresholds:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.

The System Information page displays.

5. Select System > Management > System CPU Status > CPU Threshold.

6. Specify the thresholds:
   • Rising Threshold. Notification is generated when the total CPU utilization exceeds this threshold value over the configured time period. The range is 1 to 100.
   • Rising Interval. This utilization monitoring time period can be configured from 5 to 86400 seconds in multiples of 5 seconds.
   • Falling Threshold. Notification is triggered when the total CPU utilization falls below this level for a configured period of time.
     The falling utilization threshold must be equal to or less than the rising threshold value. The falling utilization threshold notification is sent only if a rising threshold notification was sent previously. Configuring the falling utilization threshold and time period is optional. If the Falling CPU utilization settings are not configured, the switch uses the same values as the values that are used for the Rising CPU utilization. The range is 1 to 100.
   • Falling Interval. The utilization monitoring time period can be configured from 5 seconds to 86400 seconds in multiples of 5 seconds.
   • Free Memory Threshold. The free memory threshold value for the CPU in KB.

7. Click the Apply button.
   Your settings are saved.
Configure the IP Network and VLAN Settings for the Local Browser Interface

You can configure network information for the local browser 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 settings 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 configure the IP network and VLAN settings for the local browser interface:

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   - The login window opens.
4. Enter the switch’s password in the Password field.
   - The default password is password.
   - The System Information page displays.
5. Select System > Management > IP Configuration.
   - The IP Configuration page displays.
6. Select one of the following radio buttons to specify how the network information for the switch must be configured:
   - **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.
   - **Dynamic IP Address (BOOTP).** Specifies that the switch must obtain the IP address through a BootP server.
   - **Dynamic IP Address (DHCP).** Specifies that the switch must obtain the IP address through a DHCP server.
7. If you select the Static IP Address radio button, configure the following network information:
   - **IP Address.** The IP address of the network interface. The 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 default value is 255.255.255.0.
   - **Default Gateway.** The default gateway for the IP interface. The default value is 192.168.0.254.
8. To change the management VLAN, specify the VLAN ID for the new management VLAN.

The management VLAN is used to establish an IP connection to the switch from a computer that is connected to a port in the same VLAN. By default, the management VLAN ID is 1, which allows an IP connection to be established through any port.

When you change the management VLAN, an IP connection can be made only through a port that is part of the management VLAN. Also, the port VLAN ID (PVID) of the port to be connected in that management VLAN must be the same as the management VLAN ID.

The switch can automatically apply the required settings that are associated with changing the management VLAN. For more information about changing the management VLAN, see Change the Management VLAN on page 41.

9. Click the Apply button.

Your settings are saved.

Change the Management VLAN

You can let the switch change its management VLAN automatically or you can change the VLAN manually.

The following requirements apply to the management VLAN:

- Only one management VLAN can be active at a time.
- When you change the management VLAN, connectivity through the existing management VLAN is lost.
- You must connect your management computer to a port in the new management VLAN.

Change the Management VLAN Automatically

To let the switch change the management VLAN automatically, change the existing management VLAN to a new management VLAN (see Configure the IP Network and VLAN Settings for the Local Browser Interface on page 40), even if you are creating a new VLAN in the process. The switch automatically assigns the new management VLAN to all ports and PVIDs that the current management VLAN is associated with. You do not need to change any network cables.

Change the Management VLAN Manually

To change the management VLAN manually, you must take the following high-level steps:

1. Create a new VLAN that you want to use as the management VLAN (see Add a VLAN on page 123).
2. Assign the new VLAN to a port (see Configure VLAN Membership on page 125) and to the PVID for that port (see Configure Port PVID Settings on page 129).
3. Change the existing management VLAN to the new VLAN (see Change the Management VLAN on page 41).
4. Connect the network cable to the switch port that is assigned to new VLAN.
Configure the Time Settings

The switch supports the Simple Network Time Protocol (SNTP). As its name suggests, it is a less complicated version of Network Time Protocol, which is a system for synchronizing the clocks of networked computer systems, primarily when data transfer is handled through the Internet. You can also set the system time manually.

Configure the Time Setting Manually
You can view and adjust date and time settings.

To manually configure the time setting:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select System > Management > Time > Time Configuration.

6. Select the Clock Source Local radio button.

7. In the Date field, specify the current date by entering the month, day, and year (MM/DD/YYYY).

8. In the Time field, specify the current time by entering in hours, minutes, and seconds (HH:MM:SS).

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

9. Click the Apply button.
   Your settings are saved.
Configure the Time Settings With SNTP and Configure the Global SNTP Settings

To configure the time by using SNTP and configure the global SNTP settings:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.

   The System Information page displays.

5. Select System > Management > Time > Time Configuration.

   The Time Configuration page displays.

6. Select the Clock Source SNTP radio button.

   The switch can set its local clock to SNTP only if the following two conditions are met:

   • You configured the settings for an SNTP server. (For a unicast SNTP server, see Configure an SNTP Server on page 47).
   • The switch can contact the SNTP server.
7. Next to Client Mode, select the mode of operation of the SNTP client:
   • **Unicast.** SNTP operates in a point-to-point way. A unicast client sends a request to a
designated server at its unicast address and expects a reply from which it can
determine the time and, optionally, the round-trip delay and local clock offset relative
to the server.
   • **Broadcast.** SNTP operates in the same manner as multicast mode but uses a local
broadcast address instead of a multicast address. The broadcast address provides a
single-subnet scope while a multicast address provides an Internet-wide scope.

The default value is Disable.

8. If the SNTP client mode is **Unicast**, you must add the IP address or DNS name of one or
   more SNTP servers that the switch can poll.

   For more information, see Configure an SNTP Server on page 47.

9. In the **Port** field, specify the local UDP port that the SNTP client receives server packets on.

   The allowed range is 1025 to 65535 and 123. The default value is 123. When the default
   value is configured, the actual client port value used in SNTP packets is assigned by the
   switch.

10. In the **Unicast Poll Interval** field, specify the number of seconds between unicast poll
     requests expressed as a power of 2. The allowed range is 6 to 10. The default value is 6.

11. In the **Broadcast Poll Interval** field, specify the number of seconds between broadcast poll
     requests expressed as a power of 2.

     Broadcasts received prior to the expiry of this interval are discarded. The allowed range is
     6 to 10. The default value is 6.

12. In the **Unicast Poll Timeout** field, specify the number of seconds to wait for an SNTP
     response to a unicast poll request.

     The allowed range is 1 to 30. The default value is 5.

13. In the **Unicast Poll Retry** field, specify the number of times to retry a unicast poll request to
     an SNTP server after the first time-out before the switch attempts to use the next configured
     server.

     The allowed range is 0 to 10. The default value is 1.

14. In the **Time Zone Name** field, specify the acronym for a time zone.

     You can also specify the number of hours and number of minutes that the time zone is
different from the Coordinated Universal Time (UTC). The time zone can affect the
display of the current system time. The default value is UTC.

     **Note:** When you use an SNTP or NTP time server to update the switch’s
     clock, the time data received from the server is based on the UTC,
     which is the same as Greenwich Mean Time (GMT). However, this
     might not be the time zone in which the switch is located.

15. In the **Offset Hours** field, specify the number of hours that the time zone is different from the
     UTC.
For more information see the description for Time Zone Name in Step 14. The allowed range is –12 to 13. The default value is 0.

16. In the Offset Minutes field, specify the number of minutes that the time zone is different from UTC.

For more information see the description for Time Zone Name in Step 14. The allowed range is 0 to 59. The default value is 0.

17. Click the Apply button.

Your settings are saved.

View the SNTP Global Status
When you select the SNTP option as the clock source, you can view the SNTP global status.

To view the SNTP global status:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
5. Select System > Management > Time > Time Configuration.
6. Make sure that the Clock Source SNTP radio button is selected.
   The SNTP Global Status section displays below the SNTP Global Configuration section.
7. Click the **Refresh** button to refresh the page with the latest information about the switch.

The following table displays the nonconfigurable SNTP Global Status information.

**Table 10. SNTP Global Status information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>The SNTP version that the client supports.</td>
</tr>
<tr>
<td>Supported Mode</td>
<td>The SNTP modes that the client supports. Multiple modes can be supported by a client.</td>
</tr>
<tr>
<td>Last Update Time</td>
<td>The local date and time (UTC) that the SNTP client last updated the system clock.</td>
</tr>
<tr>
<td>Last Attempt Time</td>
<td>The local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.</td>
</tr>
</tbody>
</table>
| Last Attempt Status    | The status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message was received from a server, a status of **Other** is displayed. These values are appropriate for all operational modes.
  
  - **Other**: The status of the last request is unknown.
  
  - **Success**: The SNTP operation was successful and the system time was updated.
  
  - **Request Timed Out**: After an SNTP request was sent to an SNTP server, the response timer expired before a response from the server was received.
  
  - **Bad Date Encoded**: The time provided by the SNTP server is not valid.
  
  - **Version Not Supported**: The SNTP version supported by the server is not compatible with the version supported by the client.
  
  - **Server Unsynchronized**: The SNTP server is not synchronized with its peers. This is indicated by the leap indicator field in the SNTP message.
  
  - **Server Kiss Of Death**: 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.
| Server IP Address      | The IP address of the server for the last received valid packet. If no message was received from any server, an empty string is shown. |
| Address Type           | The address type of the SNTP server address for the last received valid packet. |
Configure an SNTP Server

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

Time sources are established by strata. Strata 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 strata:

- **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, through 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 that the original request was sent by the client.
- **T2.** Time that the original request was received by the server.
- **T3.** Time that the server sent a reply.
- **T4.** Time that 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 were 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

---

Table 10. SNTP Global Status information (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Stratum</td>
<td>The claimed stratum of the server for the last received valid packet.</td>
</tr>
<tr>
<td>Reference Clock ID</td>
<td>The reference clock identifier of the server for the last received valid packet.</td>
</tr>
<tr>
<td>Server mode</td>
<td>The mode of the server for the last received valid packet.</td>
</tr>
<tr>
<td>Unicast Server Max Entries</td>
<td>The maximum number of unicast server entries that can be configured on this client.</td>
</tr>
<tr>
<td>Unicast Server Current Entries</td>
<td>The number of current valid unicast server entries configured for this client.</td>
</tr>
<tr>
<td>Broadcast Count</td>
<td>The number of unsolicited broadcast SNTP messages that were received and processed by the SNTP client since the last reboot.</td>
</tr>
</tbody>
</table>
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.

You can view and modify information for adding and modifying Simple Network Time Protocol SNTP servers.

Add an SNTP Server

To add an SNTP server:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select System > Management > Time > SNTP Server Configuration.

   ![](snntp-server-configuration.png)

   The previous figure shows one server example.

6. From the Server Type menu, select the type of SNTP address to enter in the address field.
   The address can be either an IP address (IPv4) or a host name (DNS).

7. In the Address field, specify the IP address or the host name of the SNTP server.
   This is a text string of up to 64 characters, containing the encoded unicast IP address or host name of an SNTP server. Unicast SNTP requests are sent to this address. If this
address is a DNS host name, then that host name is resolved into an IP address each time an SNTP request is sent to it.

8. If the UDP port on the SNTP server to which SNTP requests are sent is not the standard port (123), specify the port number in the **Port** field.

   The range is from 1 to 65535. The default value is 123.

9. In the **Priority** field, specify the priority order which to query the servers.

   The SNTP client on the device continues sending SNTP requests to different servers until a successful response is received, or all servers are exhausted. The priority indicates the order in which to query the servers. The request is sent to an SNTP server with a priority value of 1 first, then to a server with a priority value of 2, and so on. If any servers are assigned the same priority, the SNTP client contacts the servers in the order that they appear in the table. The range is from 1 to 3. The default value is 1.

10. In the **Version** field, specify the NTP version running on the server.

    The range is 1 to 4. The default value is 4.

11. Click the **Add** button.

    The SNTP server entry is added.

12. Repeat the previous steps to add additional SNTP servers.

    You can configure up to three SNTP servers.

The SNTP Server Status table displays status information about the SNTP servers configured on your switch. The following table describes the SNTP Server Global Status information.

**Table 11. SNTP Server Status information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>All the existing server addresses. If no server configuration exists, a message stating that no SNTP server exists displays on the page.</td>
</tr>
<tr>
<td>Last Update Time</td>
<td>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>The local date and time (UTC) that this SNTP server was last queried.</td>
</tr>
</tbody>
</table>
Change the Settings for an Existing SNTP Server

To change the settings for an existing SNTP server:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select System > Management > Time > SNTP Server Configuration.
   The SNTP Server Configuration page displays.

6. Select the check box next to the configured server.

7. Specify new values in the available fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Attempt Status</td>
<td>The status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message was received from a server, a status of Other is displayed:</td>
</tr>
<tr>
<td></td>
<td>• Other. The status of the last request is unknown, or no SNTP responses were received.</td>
</tr>
<tr>
<td></td>
<td>• Success. The SNTP operation was successful and the system time was updated.</td>
</tr>
<tr>
<td></td>
<td>• Request Timed Out. After an SNTP request was sent to an SNTP server, the response timer expired before a response from the server was received.</td>
</tr>
<tr>
<td></td>
<td>• Bad Date Encoded. The time provided by the SNTP server is not valid.</td>
</tr>
<tr>
<td></td>
<td>• Version Not Supported. The SNTP version supported by the server is not compatible with the version supported by the client.</td>
</tr>
<tr>
<td></td>
<td>• Server Unsynchronized. The SNTP server is not synchronized with its peers. This is indicated by the leap indicator field on the SNTP message.</td>
</tr>
<tr>
<td></td>
<td>• Server Kiss Of Death. 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>
</tbody>
</table>

| Requests               | The number of SNTP requests made to this server since last agent reboot.                                                                      |
| Failed Requests        | The number of failed SNTP requests made to this server since the last reboot.                                                                  |
8. Click the **Apply** button.
   Your settings are saved.

Remove an SNTP Server

**To remove an SNTP server:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address** on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **System > Management > Time > SNTP Server Configuration**.
   The SNTP Server Configuration page displays.

6. Select the check box next to the configured server to remove.

7. Click the **Delete** button.
   The entry is removed, and the device is updated.

Configure Daylight Saving Time Settings

You can configure settings for summer time, which is also known as daylight saving time. Used in some countries around the world, summer time is the practice of temporarily advancing clocks during the summer months. Typically clocks are adjusted forward one or more hours near the start of spring and are adjusted backward in autumn.

**To configure the daylight saving time settings:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address** on page 12.
   The login window opens.
4. Enter the switch’s password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **System > Management > Time > DayLight Saving Configuration**.

   ![DayLight Saving Configuration](image)

6. Select a Daylight Saving (DST) radio button:
   - **Disable**. Disable daylight saving time.
   - **Recurring**. Daylight saving time occurs at the same time every year. The start and end times and dates for the time shift must be manually configured.
   - **Recurring EU**. The system clock uses the standard recurring summer time settings used in countries in the European Union. When this option is selected, the rest of the applicable fields on the page are automatically populated and cannot be edited.
   - **Recurring USA**. The system clock uses the standard recurring daylight saving time settings used in the United States. When this option is selected, the rest of the applicable fields on the page are automatically populated and cannot be edited.
   - **Non Recurring**. Daylight saving time settings are in effect only between the start date and end date of the specified year. When this option is selected, the summer time settings do not repeat on an annual basis.

7. Depending on your selection, configure the additional fields:
   - If you select the DayLight Saving (DST) **Recurring**, **Recurring EU**, or **Recurring USA** radio button, the fields in the following table are visible and you must configure them.

   **Table 12. Daylight saving setting is Recurring, Recurring EU, or Recurring USA**
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Begins At</td>
<td>These fields are used to configure the start values of the date and time.</td>
</tr>
<tr>
<td>Week</td>
<td>Configure the start week in the month.</td>
</tr>
<tr>
<td>Day</td>
<td>Configure the start day in the week.</td>
</tr>
<tr>
<td>Month</td>
<td>Configure the start month.</td>
</tr>
<tr>
<td>Hours</td>
<td>Configure the start hour.</td>
</tr>
<tr>
<td>Minutes</td>
<td>Configure the start minutes.</td>
</tr>
</tbody>
</table>
If you select the DayLight Saving (DST) Non Recurring radio button, the fields in the following table are visible and you must configure them.

**Table 13. Daylight saving setting is Non Recurring**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Begins At | These fields are used to configure the start values of the date and time.  
  • Month. Configure the start month.  
  • Date. Configure the start date in the month.  
  • Year. Configure the start year.  
  • Hours. Configure the start hour.  
  • Minutes. Configure the start minutes. |
| Ends At | These fields are used to configure the end values of date and time.  
  • Month. Configure the end month.  
  • Date. Configure the end date in the month.  
  • Year. Configure the end year.  
  • Hours. Configure the end hour.  
  • Minutes. Configure the end minutes. |
| Offset | Specify the number of minutes to shift the summer time from the standard time.  
  The range is from 1 to 1440 minutes. |
| Zone | Specify the acronym associated with the time zone when summer time is in effect. This field is not validated against an official list of time zone acronyms. |

8. Click the **Apply** button.

Your settings are saved.

**View the DayLight Saving Time Status**

The Daylight Saving (DST) Status section shows information about the summer time settings and whether the time shift for summer time is currently in effect.
To view the daylight saving time status:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.

   The System Information page displays.

5. Select System > Management > Time > DayLight Saving Configuration.

   ![DayLight Saving Configuration](image)

6. To refresh the page with the latest information about the switch, click the Refresh button.

   The following table displays the nonconfigurable daylight saving status information.

Table 14. Daylight Saving (DST) Status information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daylight Saving (DST)</td>
<td>The Daylight Saving value, which is one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Disable</td>
</tr>
<tr>
<td></td>
<td>• Recurring</td>
</tr>
<tr>
<td></td>
<td>• Recurring EU</td>
</tr>
<tr>
<td></td>
<td>• Recurring USA</td>
</tr>
<tr>
<td></td>
<td>• Non Recurring</td>
</tr>
<tr>
<td>Begins At</td>
<td>The start date of daylight saving time. This field is not displayed when</td>
</tr>
<tr>
<td></td>
<td>daylight saving time is disabled.</td>
</tr>
</tbody>
</table>
Configure Denial of Service Settings

You can configure the Denial of Service (DoS) settings for the switch. The switch provides support for classifying and blocking specific types of DoS attacks.

Configure Auto-DoS

You can automatically enable all the DoS features available on the switch, except for the L4 Port attack. For information about the types of DoS attacks the switch can monitor and block, see Configure Denial of Service on page 56.

To enable the Auto-DoS feature:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the Password field.

   The default password is password.

   The System Information page displays.

5. Select System > Management > Denial of Service > Auto-DoS Configuration.

   The Auto-DoS Configuration page displays.

6. Select the Auto-DoS Mode Enable radio button.

   When an attack is detected, a warning message is logged to the buffered log and is sent to the syslog server. At the same time, the port is shut down and can be enabled only manually by the admin user.

---

Table 14. Daylight Saving (DST) Status information (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ends At</td>
<td>The end date of daylight saving time. This field is not displayed when daylight saving time is disabled.</td>
</tr>
<tr>
<td>Offset (in Minutes)</td>
<td>The offset value in minutes. This field is not displayed when daylight saving time is disabled.</td>
</tr>
<tr>
<td>Zone</td>
<td>The zone acronym. This field is not displayed when daylight saving time is disabled.</td>
</tr>
<tr>
<td>Daylight Saving (DST) in Effect</td>
<td>Indicates whether daylight saving time is in effect.</td>
</tr>
</tbody>
</table>
7. Click the **Apply** button.  
    Your settings are saved.

**Configure Denial of Service**
You can select which types of DoS attacks the switch monitors and blocks.

**To configure individual DoS settings:**

1. Connect your computer to the same network as the switch.  
    You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.  
    If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.  
    The login window opens.

4. Enter the switch’s password in the **Password** field.  
    The default password is **password**.  
    The System Information page displays.

5. Select **System > Management > Denial of Service > Denial of Service Configuration**.
6. Select the types of DoS attacks for the switch to monitor and block and configure any associated values:

- **Denial of Service Min TCP Header Size.** Specify the minimum TCP header size allowed. If DoS TCP Fragment is enabled, the switch drops packets with a TCP header smaller than the configured value. The default value is 20.

- **Denial of Service ICMPv4.** Enabling ICMPv4 DoS prevention causes the switch to drop ICMPv4 packets with a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv4 packet size.

- **Denial of Service Max ICMPv4 Packet Size.** Specify the maximum ICMPv4 packet size allowed. If ICMPv4 DoS prevention is enabled, the switch drops IPv4 ICMP ping packets with a size greater than the configured value. The default value is 512.

- **Denial of Service ICMPv6.** Enabling ICMPv6 DoS prevention causes the switch to drop ICMPv6 packets with a type set to ECHO_REQ (ping) and a size greater than the configured ICMPv6 packet size.

- **Denial of Service Max ICMPv6 Packet Size.** Specify the maximum ICMPv6 packet size allowed. If ICMPv6 DoS prevention is enabled, the switch drops IPv6 ICMP ping packets with a size greater than the configured value. The default value is 512.

- **Denial of Service First Fragment.** Enabling First Fragment DoS prevention causes the switch to check DoS options for the first-fragment IP packets if the switch receives fragmented IP packets. Otherwise, the switch ignores the first-fragment IP packets.

- **Denial of Service ICMP Fragment.** Enabling ICMP Fragment DoS prevention causes the switch to drop ICMP fragmented packets.

- **Denial of Service Smurf.** Enabling Smurf DoS prevention causes the switch to drop broadcast ICMP echo request packet.

- **Denial of Service SIP=DIP.** Enabling SIP=DIP DoS prevention causes the switch to drop packets with a source IP address equal to the destination IP address.

- **Denial of Service SMAC=DMAC.** Enabling SMAC=DMAC DoS prevention causes the switch to drop packets with a source MAC address equal to the destination MAC address.

- **Denial of Service TCP FIN&URG&PSH.** Enabling TCP FIN & URG & PSH DoS prevention causes the switch to drop packets with TCP flags FIN, URG, and PSH set and the TCP sequence number equal to 0.

- **Denial of Service TCP Flag&Sequence.** Enabling TCP Flag DoS prevention causes the switch to drop packets with TCP control flags set to 0 and the TCP sequence number set to 0.

- **Denial of Service TCP Fragment.** Enabling TCP Fragment DoS prevention causes the switch to drop packets with a TCP payload for which the IP payload length minus the IP header size is less than the minimum allowed TCP header size.

- **Denial of Service TCP Offset.** Enabling TCP Offset DoS prevention causes the switch to drop packets with a TCP header offset set to 1.

- **Denial of Service TCP Port.** Enabling TCP Port DoS prevention causes the switch to drop packets for which the TCP source port is equal to the TCP destination port.
• **Denial of Service TCP SYN.** Enabling TCP SYN DoS prevention causes the switch to drop packets with TCP flags set.

• **Denial of Service TCP SYN&FIN.** Enabling TCP SYN & FIN DoS prevention causes the switch to drop packets with TCP flags SYN and FIN set.

• **Denial of Service UDP Port.** Enabling UDP Port DoS prevention causes the switch to drop packets for which the UDP source port is equal to the UDP destination port.

7. Click the **Apply** button.
   
   Your settings are saved.

### Configure DNS Settings

You can configure information about DNS servers that the network uses and how the switch operates as a DNS client.

**Configure Global DNS Settings and Add a DNS Server**

You can configure global DNS settings and DNS server information.

**To configure the global DNS settings and add a DNS server:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address** on page 12.
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.
   
   The System Information page displays.

5. Select **System > Management > DNS > DNS Configuration.**
6. Select the **Disable** or **Enable** radio button to specify whether to disable or enable the administrative status of the DNS client.
   - **Enable**. Allows the switch to send DNS queries to a DNS server to resolve a DNS domain name. The DNS is enabled by default.
   - **Disable**. Prevents the switch from sending DNS queries.

7. In the **DNS Default Name** field, enter the default DNS domain name to include in DNS queries.
   When the system is performing a lookup on an unqualified host name, this field is provides 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). The name must not be longer than 255 characters.

8. In the **DNS Server** field, specify the IPv4 address to which the switch sends DNS queries.

9. Click the **Add** button.
   The server is added to the list. You can specify up to eight DNS servers. The Preference field displays the server preference order. The preference is set in the order in which preferences were entered.

10. Click the **Apply** button.
    Your settings are saved.

The following table displays DNS Server Configuration information.

**Table 15. DNS Server Configuration information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The identification of the DNS Server.</td>
</tr>
<tr>
<td>Preference</td>
<td>Shows the preference of the DNS server. The preferences are determined by the order in which they were entered.</td>
</tr>
</tbody>
</table>
Remove a DNS Server
You can remove a DNS server that you no longer need.

To remove a DNS server:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or
   connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP
   Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
5. Select System > Management > DNS > DNS Configuration.
6. In the DNS Server Configuration table, select the check box for the DNS server.
   Note: If you do not select a DNS server, all the DNS servers are removed
   after you click the Delete button.
7. Click the Delete button.
   The DNS server is removed.

Configure and View Host Name-to-IP Address Information
You can manually map host names to IP addresses or view dynamic host mappings.

Add a Static Entry to the Dynamic Host Mapping Table

To add a static entry to the local dynamic host mapping table:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or
   connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP
   Address on page 12.
   The login window opens.
4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **System > Management > DNS > Host Configuration**.
   The DNS Host Configuration page displays.

6. In the **Host Name (1 to 255 characters)** field, specify the static host name to add.
   Its length cannot exceed 255 characters and it is a required field.

7. In the **IPv4/IPv6 Address** field, enter the IP address to associate with the host name.

8. Click the **Add** button.
   Your settings are saved. The entry displays in the Dynamic Host Mapping table.

Remove an Entry From the Dynamic Host Mapping Table

**To remove an entry from the Dynamic Host Mapping table:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or
   connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address on page 12**.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **System > Management > DNS > Host Configuration**.
   The DNS Host Configuration page displays.

6. Select the check box next to the entry to remove.

7. Click the **Delete** button.
   The entry is removed from the Dynamic Host Mapping table.
Change the Host Name or IP Address in an Entry of the Dynamic Host Mapping Table, View All Entries, or Clear All Entries

To change the host name or IP address in an entry of the Dynamic Host Mapping table, view all entries, or clear all entries

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select System > Management > DNS > Host Configuration.
   The DNS Host Configuration page display.

6. Select the check box next to the entry to update.

7. Enter the new information in the appropriate field.

8. Click the Apply button.
   Your settings are saved.

9. To clear all the dynamic host name entries from the list, click the Clear button.

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

Table 16.  Dynamic Host Mapping information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Lists the host name that you assign to the specified IP address.</td>
</tr>
<tr>
<td>Total</td>
<td>Time since the dynamic entry was first added to the table.</td>
</tr>
<tr>
<td>Elapsed</td>
<td>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>
Configure Green Ethernet Settings

You can configure the green Ethernet features to reduce power consumption.

To configure the Green Ethernet settings:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select System > Management > Green Ethernet > Green Ethernet Configuration.

6. Select the Auto Power Down Mode Disable or Enable radio button.
   By default, this mode is disabled. When a port link is down, the underlying physical layer goes down for a short period and then checks for port link pulses again so that auto-negotiation remains possible. In this way, the switch saves power when no link partner is present for the port.

7. Select the EEE Mode Disable or Enable radio button.
   By default, this mode is disabled. Energy Efficient Ethernet (EEE) combines the MAC with a family of physical layers that support operation in a low power mode. It is defined by the IEEE 802.3az standard. Lower power mode enables both the send and receive sides of the link to disable some functionality for power savings when the load is light. Transition to low power mode does not change the link status. Frames in transit are not dropped or corrupted in transition to and from low power mode. Transition time is transparent to upper layer protocols and applications.

8. Click the Apply button.
   Your settings are saved.
Configure Green Ethernet Interface Settings
You can configure Green Ethernet settings for individual interfaces.

**To configure the Green Ethernet interface settings:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address** on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **System > Management > Green Ethernet > Green Ethernet Interface Configuration**.

6. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.

7. From the **Auto Power Down Mode** menu, select **Enable** or **Disable**.
   By default, this mode is disabled for the port. When a port link is down, the underlying physical layer goes down for a short period and then checks for port link pulses again so that auto-negotiation remains possible. In this way, the switch saves power when no link partner is present for the port.
8. From the **EEE mode** menu, select **Enable** or **Disable**.

By default, this mode is disabled for the port. Energy Efficient Ethernet (EEE) combines the MAC with a family of physical layers that support operation in a low power mode. It is defined by the IEEE 802.3az standard. Lower power mode enables both the send and receive sides of the link to disable some functionality for power savings when the load is light. Transition to low power mode does not change the link status. Frames in transit are not dropped or corrupted in transition to and from low power mode. Transition time is transparent to upper layer protocols and applications.

9. Click the **Apply** button.

Your settings are saved.

Configure Green Ethernet Local Devices and View or Clear Device Information

You can view detailed per-port green Ethernet information and enable or disable green Ethernet settings on a single port. Using the green Ethernet features allows for power consumption savings.

**To configure green Ethernet local devices and view or clear device information:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.
   
   The System Information page displays.

5. Select **System > Management > Green Ethernet > Green Ethernet Details**.
6. From the **Interface** menu, select the interface.

7. From the **Energy Detect Admin Mode** menu, select **Enable** or **Disable**.
   
   By default, this mode is disabled for the port. When you enable this mode, and is the port link goes down, the underlying physical layer goes down for a short period and then checks for port link pulses again so that auto-negotiation remains possible. In this way, the switch saves power when no link partner is present for the port. If Energy Detect Admin Mode is not supported, N/A is displayed.

8. From the **EEE Admin mode** menu, select **Enable** or **Disable**.

   By default, this mode is disabled for the port. When you enable this mode, the port transitions to low power mode during a link idle condition. If the EEE Admin Mode is not supported, N/A is displayed.

9. In the **EEE Transmit Idle Time** field, enter the time after which switch transitions to the LPI state.

   The range is 600 to 4294967295. The default value is 600.

10. In the **EEE Transmit Wake Time** field, enter the time that the switch must wait before it transitions to the active state after it receives a packet for transmission.

    The range is 8 to 65535. The default value is 17.
11. Click the **Apply** button.
   Your settings are saved.

12. To refresh the page with the latest information about the switch, click the **Refresh** button.
13. To clear the device information, resetting all statistics for the selected interface to default values, click the **Clear** button.

The following table describes the nonconfigurable fields.

**Table 17. Green Ethernet Local Device Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cumulative EnergySaved on this port due to Green mode(s) (Watts * Hours)</td>
<td>The cumulative energy in watts multiplied by hours that is saved through the green modes that are enabled on this port.</td>
</tr>
<tr>
<td>Rx Low Power Idle Event Count</td>
<td>The number of Rx low-power idle (LPI) events since the EEE counters were cleared. The counter increments each time that the MAC Rx enters the LPI state.</td>
</tr>
<tr>
<td>Rx Low Power Idle Duration (uSec)</td>
<td>The duration of the Rx LPI state since the EEE counters were cleared. The duration of the Rx LPI state is displayed in 10 uSec increments.</td>
</tr>
<tr>
<td>Tx Low Power Idle Event Count</td>
<td>The number of Tx LPI events since the EEE counters were cleared. The counter increments each time that the MAC Tx enters the LPI state.</td>
</tr>
<tr>
<td>Tx Low Power Idle Duration (uSec)</td>
<td>The duration of the Tx LPI state since the EEE counters were cleared. The duration of the Tx LPI state is displayed in 10 uSec increments.</td>
</tr>
<tr>
<td>Tw_sys_tx (uSec)</td>
<td>The value in uSecs of Tw_sys that the switch can support.</td>
</tr>
<tr>
<td>Tw_sys_tx Echo (uSec)</td>
<td>The remote system's transmitted Tw_sys in uSecs that was used by the switch to compute the Tw_sys in requests to the remote system.</td>
</tr>
<tr>
<td>Tw_sys_rx (uSec)</td>
<td>The value of Tw_sys in uSecs that the switch requests from the remote system.</td>
</tr>
<tr>
<td>Tw_sys_rx Echo (uSec)</td>
<td>The remote system's received Tw_sys in uSecs that was used by the switch to compute the Tw_sys that it can support.</td>
</tr>
<tr>
<td>Fallback Tw_sys (uSec)</td>
<td>The value in uSecs of the fallback Tw_sys that the switch requests from the remote system.</td>
</tr>
<tr>
<td>Tx_dll_enabled</td>
<td>Indicates the initialization status of the EEE transmit Data Link Layer management function on the switch.</td>
</tr>
<tr>
<td>Tx_dll_ready</td>
<td>Indicates whether the Data Link Layer is ready and the Tx system initialization is complete and ready to update or receive LLD PDUs containing EEE TLVs.</td>
</tr>
<tr>
<td>Rx_dll_enabled</td>
<td>Indicates the status of the EEE capability negotiation on the switch.</td>
</tr>
<tr>
<td>Rx_dll_ready</td>
<td>Indicates whether the Data Link Layer is ready and the Rx system initialization is complete and ready to update or receive LLD PDUs containing EEE TLVs.</td>
</tr>
<tr>
<td>Time Since Counters Last Cleared</td>
<td>The period since the counters were cleared or the switch was powered up.</td>
</tr>
</tbody>
</table>
View Green Ethernet Information for Remote Devices

**To view green Ethernet information for remote device:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is **password**.
   
   The System Information page displays.

5. Select System > Management > Green Ethernet > Green Ethernet Details.
   
   The Green Ethernet Details page displays.


```
Remote Device Information

Interface: g1
No LLDP data has been received on this interface.
```

7. Select the interface.

The following table describes the nonconfigurable fields.

### Table 18. Green Ethernet Remote Device Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote ID</td>
<td>The remote client identifier that is assigned to the remote system.</td>
</tr>
<tr>
<td>Remote Tw_sys_tx (uSec)</td>
<td>The value in uSecs of the Tw_sys that the remote system can support.</td>
</tr>
<tr>
<td>Remote Tw_sys_tx Echo (uSec)</td>
<td>The value in uSecs of the Transmit Tw_sys that is echoed back by the remote system.</td>
</tr>
<tr>
<td>Remote Tw_sys_rx (uSec)</td>
<td>The value in uSecs of the Tw_sys that the remote system requests from the switch.</td>
</tr>
<tr>
<td>Remote Tw_sys_rx Echo (uSec)</td>
<td>The value in uSecs of the Receive Tw_sys echoed back by the remote system.</td>
</tr>
<tr>
<td>Remote Fallback Tw_sys (uSec)</td>
<td>The value in uSecs of the fallback Tw_sys that the remote system is advertising.</td>
</tr>
</tbody>
</table>
View the Green Ethernet Statistics Summary
This page summarizes the green Ethernet settings currently in use.

**To view the green Ethernet statistics:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see *Discover or Change the Switch IP Address* on page 12.
   The login window opens.
4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.
5. Select **System > Management > Green Ethernet > Green Ethernet Summary**.

   ![Green Ethernet Statistics Summary](image)

6. To refresh the page with the latest information about the switch, click the **Refresh** button.
The following table describes the nonconfigurable fields.

**Table 19. Green Ethernet Statistics Summary information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Green Ethernet Statistics Summary</strong></td>
<td></td>
</tr>
<tr>
<td>Current Power Consumption (mW)</td>
<td>The estimated power consumption by all ports of the switch in mWatts.</td>
</tr>
<tr>
<td>Percentage Power Saving (%)</td>
<td>The estimated percentage of power saved on all ports of the switch if the green modes are enabled.</td>
</tr>
<tr>
<td>Cumulative Energy Saving (W * H)</td>
<td>The estimated cumulative energy saved on the switch in watts multiplied by hours if all green modes are enabled.</td>
</tr>
<tr>
<td><strong>Green Ethernet Feature Summary</strong></td>
<td></td>
</tr>
<tr>
<td>Unit</td>
<td>The unit ID, which is always 1.</td>
</tr>
<tr>
<td>Green Features supported on this unit</td>
<td>The list of green features that are supported on the switch, which could be one or more of the following:</td>
</tr>
<tr>
<td></td>
<td>• Energy-Detect (Energy Detect)</td>
</tr>
<tr>
<td></td>
<td>• Short-Reach (Short Reach)</td>
</tr>
<tr>
<td></td>
<td>• EEE (Energy Efficient Ethernet)</td>
</tr>
<tr>
<td></td>
<td>• LPI-History (EEE Low Power Idle History)</td>
</tr>
<tr>
<td></td>
<td>• LLDP-Cap-Exchg (EEE LLDP Capability Exchange)</td>
</tr>
<tr>
<td></td>
<td>• Pwr-Usg-Est (Power Usage Estimates).</td>
</tr>
<tr>
<td><strong>Green Ethernet Interface Summary</strong></td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>The interface for which the information is displayed.</td>
</tr>
<tr>
<td>Energy Detect Admin mode</td>
<td>Indicates whether the Energy Detect mode is enabled or disabled on the port. (For more information, see Configure Green Ethernet Interface Settings on page 64).</td>
</tr>
<tr>
<td>Energy Detect Operational Status</td>
<td>Indicates the operational status of the Energy Detect mode. (For more information, see Configure Green Ethernet Interface Settings on page 64).</td>
</tr>
<tr>
<td>EEE Admin mode</td>
<td>Indicates whether the Energy Efficient Ethernet mode on the port. (For more information, see Configure Green Ethernet Interface Settings on page 64).</td>
</tr>
</tbody>
</table>

**Configure and View the Green Ethernet EEE LPI History**

You can configure and view the Green Ethernet EEE low power idle (LPI) history.

**To configure and view the port Green Ethernet EEE LPI history:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.  
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.  
   The login window opens.  

4. Enter the switch’s password in the Password field.  
   The default password is password.  
   The System Information page displays.  


6. Select the interface.  

7. In the Sampling Interval field, enter the interval at which EEE LPI data is collected.  
   This is a global setting and is applied to all interfaces. The range is from 30 to 36000 seconds. The default is 3600 seconds.  

8. In the Max Samples to keep field, enter the maximum number of samples to keep.  
   This is a global setting that is applied to all interfaces. The range is from 1 to 168. The default is 168.  

9. Click the Apply button.  
   Your settings are saved.  

10. To refresh the page with the latest information about the switch, click the Refresh button.  
    The Percentage LPI time field shows the time spent in LPI mode since EEE counters were cleared.  

The following table describes the nonconfigurable fields.  

Table 20. Interface Green Mode EEE LPI History information  

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample No.</td>
<td>The sample index number.</td>
</tr>
<tr>
<td>Time Since The Sample Was Recorded</td>
<td>The interval between the current time and the time at which the sample was recorded.</td>
</tr>
</tbody>
</table>
Use the Device View

For information about the device view, see Use the Device View of the Local Browser Interface on page 22.

Configure PoE

On model GS324TP, you can configure the global Power over Ethernet (PoE) settings and the PoE settings for each port.

**Note:** For more information about PoE, see the hardware installation guide, which you can download by visiting netgear.com/support/download/.

Configure the Global PoE Settings

**To configure the PoE settings:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.

---

Table 20. Interface Green Mode EEE LPI History information (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage Time spent in LPI mode since last sample</td>
<td>The percentage of time spent in LPI mode during the current measurement interval.</td>
</tr>
<tr>
<td>Percentage Time spent in LPI mode since last reset</td>
<td>The percentage of time spent in LPI mode since the EEE LPI statistics were reset.</td>
</tr>
</tbody>
</table>
The System Information page displays.

5. Select **System > PoE > Basic > PoE Configuration**.

![PoE Configuration Page](image)

The previous figure shows the PoE Configuration page for model GS324TP.

6. In the **System Usage Threshold** field, enter a number from 1 to 99 to set the threshold level at which a trap is sent if the consumed power exceeds the threshold power. The default is 95 percent.

7. From the **Power Management Mode** menu, select the power management algorithm that the switch uses to deliver power to the requesting powered devices (PDs):
   - **Static**. Specifies that the power allocated for each port depends on the type of power threshold configured on the port.
   - **Dynamic**. Specifies that the power consumption on each port is measured and calculated in real time. This is the default setting.

8. To active the PoE traps, select the **Enable** radio button.

   Selecting the **Disable** radio button deactivates the PoE traps. The default setting is **Enabled**.

9. Click the **Apply** button.

   Your settings are saved.

The following table describes the nonconfigurable fields on the page.

### Table 21. PoE Configuration fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware Version</td>
<td>The firmware version of the PoE firmware component.</td>
</tr>
<tr>
<td>Power Status</td>
<td>The power status.</td>
</tr>
<tr>
<td>Total Power Available Watts</td>
<td>The maximum amount of power in watts that the switch can deliver to all ports.</td>
</tr>
<tr>
<td>Threshold Power Watts</td>
<td>If the consumed power is below the threshold power, the switch can power up another port. The consumed power can be between the nominal and threshold power. The threshold power is displayed in watts.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The threshold power value is determined by the value that you enter in the System Usage Threshold field.</td>
</tr>
<tr>
<td>Consumed Power Watts</td>
<td>The total amount of power in watts that is being delivered to all ports.</td>
</tr>
</tbody>
</table>
Configure the PoE Port Settings

To configure the PoE port settings:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch's password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select System > PoE > Advanced > PoE Port Configuration.

   The previous figure shows the PoE Port Configuration page for model GS324TP.

6. Select one or more interfaces by taking one of the following actions:
   • To configure a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   • To configure multiple interfaces with the same settings, select the check box associated with each interface.
   • To configure all interfaces with the same settings, select the check box in the heading row.

7. From the Port Power menu, select the PoE mode of the port:
   • Enable. The port’s capacity to deliver power is enabled. This is the default setting.
   • Disable. The port’s capacity to deliver power is disabled.

8. From the Port Priority menu, select the priority for the port in relation to other ports if the total power that the switch is capable of delivering exceeds the total power budget:
   • Low. Low priority. This is the default setting.
   • Medium. Medium priority.
• **High.** High priority.
• **Critical.** Critical priority.

The port priority determines which ports can still deliver power after the total power delivered by the switch exceeds the total power budget. (In such a situation, the switch might not be able to deliver power to all connected devices.) If the same priority applies to two ports, the lower-numbered port receives higher priority.

9. From the **Power Mode** menu, select the PoE mode that the port must function in:
   • **802.3af.** The port is powered in and limited to the IEEE 802.3af mode. A PD that requires IEEE 802.3at does not receive power if the port functions in IEEE 802.3af mode.
   • **Legacy.** The port is powered using high-inrush current, which is used by legacy PDs that require more than 15W to power up.
   • **Pre-802.3at.** The port is initially powered in the IEEE 802.3af mode and, before 75 msec pass, is switched to the high power IEEE 802.3at mode. Select this mode if the PD does not perform Layer 2 classification or if the switch performs 2-event Layer 1 classification.
   • **802.3at.** The port is powered in the IEEE 802.3at mode and is backward compatible with IEEE 802.3af. The 802.3at mode is the default mode. In this mode, if the switch detects that the attached PD requests more power than IEEE 802.3af but is not an IEEE 802.3at Class 4 device, the PD does not receive power from the switch.

10. From the **Power Limit Type** menu, select how the port controls the maximum power that it can deliver:
    • **None.** The port draws up to Class 0 maximum power in low power mode and up to Class 4 maximum power in high power mode.
    • **Class.** The port power limit is equal to the class of the attached PD.
    • **User.** The port power limit is equal to the value that is specified in the **Power Limit (mW)** field. This is the default setting.

    **Note:** If a PD does not report its class correctly, use of these options can preserve additional PoE power by preventing the switch from delivering more power than the PD requires. However, depending on which option you select, a PD that does not report its class correctly might not power up at all.

11. In the **Power Limit (mW)** field, enter the maximum power (in mW) that the port can deliver. The range is 3,000–30,000 mW. The default is 30,000 mW.

12. From the **Detection Type** menu, select how the port detects the attached PD:
    • **IEEE 802.** The port performs a 4-point resistive detection. This is the default setting.
    • **4pt 802.3af + legacy.** The port performs a 4-point resistive detection, and if required, continues with legacy detection.
    • **legacy.** The port performs legacy detection.
13. From the Timer Schedule menu, select a timer schedule or select None, which is the default selection.

For information about setting up and configuring PoE timer schedules, see Set Up PoE Timer Schedules on page 106.

14. Click the Apply button.

Your settings are saved.

The following table describes the nonconfigurable fields on the page.

**Table 22. PoE Port Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Power</td>
<td>All ports supports high power mode.</td>
</tr>
<tr>
<td>Max Power (W)</td>
<td>The maximum power in watts that can be provided by the port.</td>
</tr>
<tr>
<td>Class</td>
<td>The class defines the range of power that a powered device (PD) is drawing from the switch. The class definitions are as follows:</td>
</tr>
<tr>
<td></td>
<td>• 0: 0.44–16.2W</td>
</tr>
<tr>
<td></td>
<td>• 1: 0.44–4.2W</td>
</tr>
<tr>
<td></td>
<td>• 2: 0.44–7.4W</td>
</tr>
<tr>
<td></td>
<td>• 3: 0.44–16.2W</td>
</tr>
<tr>
<td></td>
<td>• 4: 0.44–31.6W</td>
</tr>
<tr>
<td></td>
<td>• Unknown. The class cannot be detected, or no PD is attached to the port.</td>
</tr>
<tr>
<td>Output Voltage (Volts)</td>
<td>The voltage that is delivered to the PD in volts.</td>
</tr>
<tr>
<td>Output Current (mA)</td>
<td>The current that is delivered to the PD in mA.</td>
</tr>
<tr>
<td>Output Power (W)</td>
<td>The power that is delivered to the PD in watts.</td>
</tr>
<tr>
<td>Status</td>
<td>The operational status of the port:</td>
</tr>
<tr>
<td></td>
<td>• Disabled. No power is delivered.</td>
</tr>
<tr>
<td></td>
<td>• Delivering Power. Power is being drawn by the PD.</td>
</tr>
<tr>
<td></td>
<td>• Requesting Power. The port is requesting power.</td>
</tr>
<tr>
<td></td>
<td>• Fault. A problem occurred with the power.</td>
</tr>
<tr>
<td></td>
<td>• Test. The port is in test mode.</td>
</tr>
<tr>
<td></td>
<td>• Other Fault. The port is idle because of an error condition.</td>
</tr>
<tr>
<td></td>
<td>• Searching. The port is not in one of the other states in this list.</td>
</tr>
</tbody>
</table>
Configure SNMP

You can configure SNMP settings for SNMPv1/v2 and SNMPv3. The switch software supports the configuration of SNMP groups and users that can manage traps that the SNMP agent generates.

The switch uses both standard public MIBs for standard functionality and private MIBs that support additional switch functionality. All private MIBs begin with a hyphen (-) 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.

Configure the SNMPv1/v2 Community

Only the communities that you define can access to the switch using the SNMP V1 and SNMP V2 protocols. Only those communities with read/write level access can be used to change the configuration using SNMP.

Add an SNMP Community:

To add an SNMP community:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
The login window opens.

4. Enter the switch’s password in the Password field.

The default password is password.

The System Information page displays.

5. Select System > SNMP > SNMP V1/V2 > Community Configuration.

6. In the Management Station IP field, specify the IP address of the management station.

7. In the Management Station IP Mask field, specify the subnet mask to associate with the management station IP address.

Together, the management station IP address and the management station IP mask denote a range of IP addresses from which SNMP clients can use that community to access this device. If either the management station IP address 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. If the values are equal, access is allowed.

For example, if the management station IP address and management station IP mask settings are 192.168.1.0/255.255.255.0, any client with an IP address in the range from 192.168.1.0 to 192.168.1.255 (inclusive) is allowed access. To allow access from only one station, use a management station IP mask value of 255.255.255.255, and use that computer’s IP address as the client address.

8. In the Community String field, specify a community name.

9. From the Access Mode menu, select the access level for this community, which is either Read/Write or Read Only.

10. From the Status menu, select to enable or disable the community.

    If you select Enable, the community name must be unique among all valid community names or the set requests are rejected. If you select Disable, the community name becomes invalid.

11. Click the Add button.

    The selected community is added.

Modify an Existing SNMP Community

To modify an existing SNMP community:

1. Connect your computer to the same network as the switch.

    You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
5. Select System > SNMP > SNMP V1/V2 > Community Configuration.
   The Community Configuration page displays.
6. Select the check box next to the community.
7. Update the desired fields.
8. Click the Apply button.
   Your settings are saved.

Delete an SNMP Community

To delete an SNMP community:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
5. Select System > SNMP > SNMP V1/V2 > Community Configuration.
   The Community Configuration page displays.
6. Select the check box next to the community to remove.
7. Click the Delete button.
   The community is removed.
Configure SNMPv1/v2 Trap Settings

You can configure settings for each SNMPv1 or SNMPv2 management host that must receive notifications about traps generated by the device. The SNMP management host is also known as the SNMP trap receiver.

Add an SNMP Trap Receiver

To add an SNMP trap receiver:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select System > SNMP > SNMP V1/V2 > Trap Configuration.
   The Trap Configuration page displays.

6. In the Recipients IP field, enter the IPv4 address at which the SNMP traps from the switch must be received.

7. From the Version menu, select the trap version to be used by the SNMP trap receiver.
   • SNMPv1. The switch uses SNMPv1 to send traps to the receiver. The default setting is SNMPv1.
   • SNMPv2. The switch uses SNMPv2 to send traps to the receiver.

8. In the Community String field, specify the name of the SNMP community that includes the SNMP management host and the SNMP agent on the device.
   This name can be up to 16 characters and is case-sensitive.

9. From the Status menu, select Enable to send traps to the receiver or select Disable to prevent the switch from sending traps to the receiver.

10. Click the Add button.
    The receiver configuration is added.
Modify Information About an Existing SNMP Recipient

**To modify information about an existing SNMP recipient:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select System > SNMP > SNMP V1/V2 > Trap Configuration.
   The Trap Configuration page displays.

6. Select the check box next to the recipient.

7. Change the fields as necessary.

8. Click the Apply button.
   Your settings are saved.

Delete an SNMP Recipient

**To delete an SNMP trap recipient:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select System > SNMP > SNMP V1/V2 > Trap Configuration.
The Trap Configuration page displays.

6. Select the check box next to the recipient to remove.
7. Click the Delete button.
   The trap recipient is removed.

Configure SNMPv1/v2 Trap Flags

You can enable or disable traps that 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 configure the trap flags:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
5. Select System > SNMP > SNMP V1/V2 > Trap Flags.
   The Trap Flags page displays.
6. Enable or disable the following system traps:
   • Authentication. When enabled, SNMP traps are sent when events involving authentication occur, such as when a user attempts to access the switch local browser interface and does not provide a valid user name and password. The default is Enable.
   • Link Up/Down. When enabled, SNMP traps are sent when the administrative or operational state of a physical or logical link changes. The default is Enable.
   • Spanning Tree. When enabled, SNMP traps are sent when various spanning tree events occur. The default is Enable.
   • ACL. When enabled, SNMP traps are sent when a packet matches an ACL rule that you configured and that includes ACL logging. The default is Disable.
   • PoE (model GS324TP only). When enabled, SNMP traps are sent when a PoE event occurs. The default is Enable
7. Click the **Apply** button.
   Your settings are saved.

View the Supported MIBs

You can view a list of all MIBs that are supported on the switch.

**To view the supported MIBs:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is `password`.
   The System Information page displays.

5. Select **System > SNMP > SNMP V1/V2 > Supported MIBs**.

The following table describes the SNMP Supported MIBs Status fields.

**Table 23. SNMP supported MIBs**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The RFC number if applicable and the name of the MIB.</td>
</tr>
<tr>
<td>Description</td>
<td>The RFC title or MIB description.</td>
</tr>
</tbody>
</table>
Configure SNMP V3 Users

Any user can connect to the switch using the SNMPv3 protocol, but for authentication and encryption, the switch supports only one user (admin). Therefore, you can create or modify only one profile.

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

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select System > SNMP > SNMPv3 > User Configuration.
   The User Configuration page displays.
   The SNMPv3 Access Mode field shows the access privileges for the user account. Access for the admin account is always Read Write. Access for all other accounts is Read Only.

6. To enable authentication, select an Authentication Protocol radio button.
   You can select the MD5 radio button or the SHA radio button. With either of these options, the user login password is used as SNMPv3 authentication password. For information about how to configure the login password, see Change the Password for the Local Browser Interface on page 210.

7. To enable encryption:
   a. Select the Encryption Protocol DES radio button to encrypt SNMPv3 packets using the DES encryption protocol.
   b. In the Encryption Key field, enter an encryption code of eight or more alphanumeric characters.

8. Click the Apply button.
   Your settings are saved.
Configure 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. A network manager can view this information to identify system topology and detect bad configurations on the LAN.

The following sections describe how you can configure LLDP:

- Configure LLDP Global Settings on page 85
- Configure LLDP Port Settings on page 87
- View the LLDP-MED Network Policy on page 88
- Configure LLDP-MED Port Settings on page 90
- View the LLDP-MED Neighbors Information on page 91
- View the Local Information Advertised Through LLDP on page 93
- View LLDP Neighbors Information on page 96

LLDP is a one-way protocol without any 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 or 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:

- Autodiscovery 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).

Configure LLDP Global Settings

You can specify the global LLDP and LLDP-MED settings that are applied to the switch.

To configure global LLDP settings:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch. 
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field. 
   The default password is password.
   The System Information page displays.

5. Select System > LLDP > Basic > LLDP Configuration.

6. To configure nondefault values for the following LLDP properties, specify the following options:
   - **TLV Advertised Interval.** The number of seconds between transmissions of LLDP advertisements.
   - **Hold Multiplier.** The transmit interval multiplier value, where transmit hold multiplier \( \times \) transmit interval = the time to live (TTL) value that the device advertises to neighbors.
   - **Re-initializing Delay.** The number of seconds to wait before attempting to re-initialize LLDP on a port after the LLDP operating mode on the port changes.
   - **Transmit Delay.** The minimum number of seconds to wait between transmissions of remote data change notifications to one or more SNMP trap receivers configured on the switch.

7. To configure a nondefault value for LLDP-MED, enter a value in the Fast Start Duration field.
   This value sets 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.

8. Click the Apply button.
   Your settings are saved.
Configure LLDP Port Settings

You can specify per-interface LLDP settings.

**To configure the LLDP interface:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch's password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **System > LLDP > Advanced > LLDP Port Settings**.

![LLDP Port Settings](image)

6. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
7. Use the following menus to configure the LLDP settings for the selected ports:
   • **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.
     The default is **Tx and Rx.**

   • **Management IP Address.** Choose whether to advertise the management IP address from the interface. The possible field values are as follows:
     - **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.
     The default is **Auto Advertise.**

   • **Notification.** When notifications are enabled, LLDP interacts with the trap manager to notify subscribers of remote data change statistics. The default is **Disable.**

   • **Optional TLVs.** Enable or disable the transmission of optional type-length value (TLV) information from the interface. The default is **Enable.** The TLV information includes the system name, system description, system capabilities, and port description.

     For information about how to configure the system name, see View and Configure the Switch Management Settings on page 32. For information about how to configure the port description, see Configure the Port Settings and Maximum Frame Size on page 114.

8. Click the **Apply** button.

   Your settings are saved.

---

**View the LLDP-MED Network Policy**

You can display information about the LLPD-MED network policy TLV transmitted in the LLDP frames on the selected local interface.

**To view LLDP-MED network policy information for an interface:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
The login window opens.

4. Enter the switch’s password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **System > LLDP > Advanced > LLDP-MED Network Policy**.

   The LLDP-MED Network Policy page displays.

6. From the **Interface** menu, select the interface for which you want to view the information.

   **Note:** The menu includes only the interfaces on which LLDP is enabled. If no interfaces are enabled for LLDP, the **Interface** menu does not display.

7. To refresh the page with the latest data transmitted in the network policy TLVs for the interface, click the **Refresh** button.

The following table describes the LLDP-MED network policy information that displays on the page.

**Table 24. LLDP-MED network policy information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Policy Number</td>
<td>The policy number.</td>
</tr>
<tr>
<td>Application</td>
<td>The media application type associated with the policy, which can 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 is displayed only if a network policy TLV was transmitted from the port.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID associated with the policy.</td>
</tr>
<tr>
<td>VLAN Type</td>
<td>Indicates whether the VLAN associated with the policy is tagged or untagged.</td>
</tr>
<tr>
<td>User Priority</td>
<td>The priority associated with the policy.</td>
</tr>
<tr>
<td>DSCP</td>
<td>The DSCP associated with a particular policy type.</td>
</tr>
</tbody>
</table>
Configure LLDP-MED Port Settings

You can enable LLDP-MED mode on an interface and configure its properties.

To configure LLDP-MED settings for a port:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
5. Select System > LLDP > Advanced > LLDP-MED Port Settings.
   The LLDP-MED Port Settings page displays.
6. From the Port menu, select the port to configure.
7. Use the following menus to enable or disable the following LLDP-MED settings for the selected port:
   • LLDP-MED Status. The administrative status of LLDP-MED on the interface. When LLDP-MED is enabled, the transmit and receive function of LLDP is effectively enabled on the interface.
   • Notification. When Notification is enabled, the port sends a topology change notification if a device is connected or removed.
   • MED Capabilities. When MED Capabilities is enabled, the port transmits the capabilities type length values (TLVs) in the LLDP PDU frames.
   • Network Policy. When Network Policy is enabled, the port transmits the network policy TLV in LLDP frames.
   • Extended MDI-PSE. When Extended MDI-PSE is enabled, the port transmits the extended PSE TLV in LLDP frames.
8. Click the Apply button.
   Your settings are saved.
View the LLDP-MED Neighbors Information

You can display the LLDP-MED neighbor or remote device information for an interface.

To view LLDP-MED Neighbor Information:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch's password in the **Password** field.
   
   The default password is **password**.
   
   The System Information page displays.

5. Select **System > LLDP > Advanced > LLDP-MED Neighbors Information**.
   
   The page that displays shows multiple sections with information about LLDP-MED neighbors.

6. From the **Interface** menu, select an interface.
   
   The menu includes only the interfaces for which LLDP is enabled.

7. To refresh the page with the latest information about the switch, click the **Refresh** button.
   
   The following table describes the non-configurable LLDP-MED Neighbors Information that displays for the selected interface.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP-MED Interface Selection</td>
<td></td>
</tr>
<tr>
<td>Remote ID</td>
<td>Specifies the remote client identifier assigned to the remote system.</td>
</tr>
<tr>
<td><strong>Capability Information</strong></td>
<td></td>
</tr>
<tr>
<td>This section of the page specifies the supported and enabled capabilities that are received in MED TLV on this port.</td>
<td></td>
</tr>
<tr>
<td>Supported Capabilities</td>
<td>Specifies supported capabilities that are received in MED TLV on this port.</td>
</tr>
<tr>
<td>Enabled Capabilities</td>
<td>Specifies enabled capabilities that are received in MED TLV on this port.</td>
</tr>
<tr>
<td>Device Class</td>
<td>Specifies device class as advertised by the device remotely connected to the port.</td>
</tr>
</tbody>
</table>
### Media Application Type

Specifies the application type: unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streamingvideo, or videosignaling.

Information for each application type includes the VLAN ID, priority, DSCP, tagged bit status and unknown bit status. A port can receive information about one or many of such application types. The application type is displayed only if a network policy TLV is received on a port.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>Specifies the VLAN ID associated with a particular policy type.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies the priority associated with a particular policy type.</td>
</tr>
<tr>
<td>DSCP</td>
<td>Specifies the DSCP associated with a particular policy type.</td>
</tr>
<tr>
<td>Unknown Bit Status</td>
<td>Specifies the unknown bit associated with a particular policy type.</td>
</tr>
<tr>
<td>Tagged Bit Status</td>
<td>Specifies the tagged bit associated with a particular policy type.</td>
</tr>
</tbody>
</table>

### Inventory Information

This section of the page specifies if inventory TLV is received in LLDP frames on this port.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Revision</td>
<td>Specifies the hardware version of the remote device.</td>
</tr>
<tr>
<td>Firmware Revision</td>
<td>Specifies the firmware version of the remote device.</td>
</tr>
<tr>
<td>Software Revision</td>
<td>Specifies software version of the remote device.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Specifies the serial number of the remote device.</td>
</tr>
<tr>
<td>Manufacturer Name</td>
<td>Specifies the manufacturer’s name of the remote device.</td>
</tr>
<tr>
<td>Model Name</td>
<td>Specifies the model name of the remote device.</td>
</tr>
<tr>
<td>Asset Id</td>
<td>Specifies the asset ID of the remote device.</td>
</tr>
</tbody>
</table>

### Location Information

This section of the page specifies if location TLV is received in LLDP frames on this port.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub Type</td>
<td>Specifies the type of location information.</td>
</tr>
<tr>
<td>Location Information</td>
<td>Specifies the location information as a string for a given type of location ID.</td>
</tr>
</tbody>
</table>

### Extended PoE

This section of the page specifies if the remote device is a PoE device.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Type</td>
<td>Specifies the remote device’s PoE device type connected to this port.</td>
</tr>
<tr>
<td>Extended PoE PSE</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Type</td>
<td>Specifies the remote device’s PoE device type connected to this port.</td>
</tr>
</tbody>
</table>
View the Local Information Advertised Through LLDP

You can view the data that each port advertises through LLDP.

**To view local LLDP information:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.

   The System Information page displays.

5. Select **System > LLDP > Advanced > Local Information**.
The page includes only the interfaces on which LLDP is enabled.

6. To refresh the page with the latest information about the switch, click the **Refresh** button.

The following table describes the LLDP device information and port summary information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Information</strong></td>
<td></td>
</tr>
<tr>
<td>Chassis ID Subtype</td>
<td>The type of information used to identify the switch in the Chassis ID field.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>The hardware platform identifier for the switch.</td>
</tr>
<tr>
<td>System Name</td>
<td>The user-configured system name for the switch.</td>
</tr>
<tr>
<td>System Description</td>
<td>The switch description, which includes information about the product model and platform.</td>
</tr>
<tr>
<td>System Capabilities</td>
<td>The primary functions that the switch supports.</td>
</tr>
<tr>
<td><strong>Port Information</strong></td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>The interface associated with the rest of the data in the row.</td>
</tr>
<tr>
<td>Port ID Subtype</td>
<td>The type of information used to identify the interface in the Port ID field.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The port number.</td>
</tr>
<tr>
<td>Port Description</td>
<td>The user-defined description of the port. For information about how to configure the port description, see <strong>Configure the Port Settings and Maximum Frame Size on page 114</strong>.</td>
</tr>
<tr>
<td>Advertisement</td>
<td>The TLV advertisement status of the port.</td>
</tr>
</tbody>
</table>

7. To view additional details about a port, click the name of the port in the Interface column of the Port Information table.
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></td>
</tr>
<tr>
<td>Address SubType</td>
<td>The type of address the management interface uses, such as an IPv4 address.</td>
</tr>
<tr>
<td>Address</td>
<td>The address used to manage the device.</td>
</tr>
<tr>
<td>Interface SubType</td>
<td>The port subtype.</td>
</tr>
<tr>
<td>Interface Number</td>
<td>The number that identifies the port.</td>
</tr>
<tr>
<td>MAC/PHY Details</td>
<td></td>
</tr>
<tr>
<td>Auto Negotiation Supported</td>
<td>Indicates whether the interface supports port speed autonegotiation. The option is True (enabled) or False (disabled).</td>
</tr>
<tr>
<td>Auto Negotiation Enabled</td>
<td>The port speed autonegotiation support status. The option is True (enabled) or False (disabled).</td>
</tr>
<tr>
<td>Auto Negotiation Advertised</td>
<td>The port speed autonegotiation capabilities such as 1000BASE-T half-duplex mode or 100BASE-TX full-duplex mode.</td>
</tr>
<tr>
<td>Capabilities</td>
<td>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>Operational MAU Type</td>
<td></td>
</tr>
<tr>
<td>MED Details</td>
<td></td>
</tr>
<tr>
<td>Capabilities Supported</td>
<td>The MED capabilities enabled on the port.</td>
</tr>
<tr>
<td>Current Capabilities</td>
<td>The TLVs advertised by the port.</td>
</tr>
<tr>
<td>Device Class</td>
<td>Network Connectivity indicates that the device is a network connectivity device.</td>
</tr>
<tr>
<td>Network Policies</td>
<td></td>
</tr>
<tr>
<td>Application Type</td>
<td>The media application type associated with the policy.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>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>The priority associated with the policy.</td>
</tr>
<tr>
<td>DSCP</td>
<td>The DSCP associated with a particular policy type.</td>
</tr>
</tbody>
</table>
View LLDP Neighbors Information

You can view the data that a specified interface received from other LLDP-enabled systems.

**To view LLDP information received from a neighbor device:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.

   The System Information page displays.

5. Select System > LLDP > Advanced > Neighbors Information.
   
   The Neighbors Information page displays.

   If no information was received from a neighbor device, or if the link partner is not LLDP-enabled, no information displays.

6. To refresh the page with the latest LLDP neighbor information, click the Refresh button.
   
   The following table describes the information that displays for all LLDP neighbors that were discovered.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSAP Entry</td>
<td>The Media Service Access Point (MSAP) entry number for the remote device.</td>
</tr>
<tr>
<td>Local Port</td>
<td>The interface on the local system that received LLDP information from a remote system.</td>
</tr>
<tr>
<td>Chassis ID Subtype</td>
<td>The type of data displayed in the Chassis ID field on the remote system.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>The remote 802 LAN device’s chassis.</td>
</tr>
<tr>
<td>Port ID Subtype</td>
<td>The type of data displayed in the remote system’s Port ID field.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The physical address of the port on the remote system from which the data was sent.</td>
</tr>
<tr>
<td>System Name</td>
<td>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>
7. To view additional information about the remote device, click the link in the MSAP Entry column.

A pop-up window displays information for the selected port.

The following table describes the information transmitted by the neighbor.

<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>The interface on the local system that received LLDP information from a remote system.</td>
</tr>
<tr>
<td>MSAP Entry</td>
<td>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>The type of data displayed in the Chassis ID field on the remote system.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>The remote 802 LAN device’s chassis.</td>
</tr>
<tr>
<td>Port ID Subtype</td>
<td>The type of data displayed in the remote system’s Port ID field.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The physical address of the port on the remote system from which the data was sent.</td>
</tr>
<tr>
<td>Port Description</td>
<td>The user-defined description of the port.</td>
</tr>
<tr>
<td>System Name</td>
<td>The system name associated with the remote device.</td>
</tr>
<tr>
<td>System Description</td>
<td>The description of the selected port associated with the remote system.</td>
</tr>
<tr>
<td>System Capabilities</td>
<td>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>The type of the management address.</td>
</tr>
<tr>
<td>Address</td>
<td>The advertised management address of the remote system.</td>
</tr>
<tr>
<td>Interface SubType</td>
<td>The port subtype.</td>
</tr>
<tr>
<td>Interface Number</td>
<td>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 autonegotiation. The option is True (enabled) or False (disabled).</td>
</tr>
<tr>
<td>Auto-Negotiation Enabled</td>
<td>The port speed autonegotiation support status. The option is True (enabled) or False (disabled).</td>
</tr>
<tr>
<td>Auto Negotiation Advertised Capabilities</td>
<td>The port speed autonegotiation capabilities.</td>
</tr>
<tr>
<td>Operational MAU Type</td>
<td>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>
### MED Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capabilities Supported</td>
<td>The supported capabilities that were received in MED TLV from the device.</td>
</tr>
<tr>
<td>Current Capabilities</td>
<td>The advertised capabilities that were received in MED TLV from the device.</td>
</tr>
<tr>
<td>Device Class</td>
<td>The LLDP-MED endpoint device class. The possible device classes are as follows:</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>The port PoE type. For example, Powered.</td>
</tr>
<tr>
<td>PoE Power Source</td>
<td>The port’s power source.</td>
</tr>
<tr>
<td>PoE Power Priority</td>
<td>The port’s power priority.</td>
</tr>
<tr>
<td>PoE Power Value</td>
<td>The port’s power value.</td>
</tr>
<tr>
<td>Hardware Revision</td>
<td>The hardware version advertised by the remote device.</td>
</tr>
<tr>
<td>Firmware Revision</td>
<td>The firmware version advertised by the remote device.</td>
</tr>
<tr>
<td>Software Revision</td>
<td>The software version advertised by the remote device.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number advertised by the remote device.</td>
</tr>
<tr>
<td>Model Name</td>
<td>The model name advertised by the remote device.</td>
</tr>
<tr>
<td>Asset ID</td>
<td>The asset ID advertised by the remote device.</td>
</tr>
</tbody>
</table>

### Location Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civic</td>
<td>The physical location, such as the street address, that the remote device 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>The location map coordinates that the remote device advertised in the location TLV, including latitude, longitude, and altitude.</td>
</tr>
<tr>
<td>ECS ELIN</td>
<td>The Emergency Call Service (ECS) Emergency Location Identification Number (ELIN) that the remote device advertised in the location TLV. The field range is 10–25.</td>
</tr>
<tr>
<td>Unknown</td>
<td>The unknown location information for the remote device.</td>
</tr>
</tbody>
</table>
Configure DHCP Snooping

DHCP snooping is a useful feature that provides security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding table. An untrusted message is a message that is received from outside the network or firewall and that can cause traffic attacks within your network. The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. It also provides way to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

Configure the Global DHCP Snooping Settings

You can view and configure the global settings for DHCP snooping.

To configure the global DHCP snooping settings:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Policies</strong></td>
<td></td>
</tr>
<tr>
<td>Application Type</td>
<td>The media application type associated with the policy advertised by the remote device.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>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>The priority associated with the policy.</td>
</tr>
<tr>
<td>DSCP</td>
<td>The DSCP associated with a particular policy type.</td>
</tr>
<tr>
<td><strong>LLDP Unknown TLVs</strong></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>The unknown TLV type field.</td>
</tr>
<tr>
<td>Value</td>
<td>The unknown TLV value field.</td>
</tr>
</tbody>
</table>
If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

The login window opens.

4. Enter the switch’s password in the **Password** field.

   The default password is **password**.

The System Information page displays.

5. Select **System** > **Services** > **DHCP Snooping** > **Global Configuration**.

![DHCP Snooping Configuration](image)

6. Select the DHCP Snooping Mode **Enable** radio button.

   The default is **Disable**.

7. To enable the verification of the sender’s MAC address for DHCP snooping, leave the MAC Address Validation **Enable** radio button selected.

   The default is **Enable**.

   When MAC address validation is enabled, the device checks packets that are received on an untrusted interface to verify that the MAC address and the DHCP client hardware address match. If the addresses do not match, the device drops the packet.

8. Click the **Apply** button.

   Your settings are saved.

---

**Enable DHCP for All Interfaces in a VLAN**

**To enable DHCP snooping for all interfaces that are members of a VLAN:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select System > Services > DHCP Snooping > Global Configuration.
   The DHCP Snooping Global Configuration page displays.

6. In the VLAN ID field, specify the VLAN on which DHCP snooping is enabled.
7. From the DHCP Snooping Mode menu, select Enable.
8. Click the Apply button.

Your settings are saved.

Configure DHCP Snooping Interface Settings

You can 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 configure DHCP snooping interface settings:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select System > Services > DHCP Snooping > Interface Configuration.
6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   • 1 (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   • LAG. Only LAGs are displayed.
   • All. Both physical interfaces and LAGs are displayed.

7. Select one or more interfaces by taking one of the following actions:
   • To configure a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   • To configure multiple interfaces with the same settings, select the check box associated with each interface.
   • To configure all interfaces with the same settings, select the check box in the heading row.

8. From the Trust Mode menu, select the desired trust mode:
   • Disabled. The interface is considered to be untrusted and could potentially be used to launch a network attack. DHCP server messages are checked against the bindings database. On untrusted ports, DHCP snooping enforces the following security rules:
     - DHCP packets from a DHCP server (DHCOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) are dropped.
     - DHCPRELEASE and DHCPDECLINE messages are dropped if the MAC address is in the snooping database but the binding’s interface is other than the interface where the message was received.
     - DHCP packets are dropped when the source MAC address does not match the client hardware address if MAC address validation is globally enabled.
   • Enabled. The interface is considered to be trusted and forwards DHCP server messages without validation.

9. From the Invalid Packets menu, select the packet logging mode.
   When enabled, the DHCP snooping feature generates a log message when an invalid packet is received and dropped by the interface.

10. In the Rate Limit (pps) field, specify the rate limit value for DHCP snooping purposes.
    If the incoming rate of DHCP packets per second exceeds the configured burst interval per second, the port shuts down. If the rate limit value is None, the burst interval is also nonapplicable, and rate limiting is disabled.

11. In the Burst Interval (secs) field, specify the burst interval value for rate limiting purposes on the interface.
    If the rate limit is N/A, then the burst interval is also nonapplicable, and the field displays N/A.

12. Click the Apply button.
    Your settings are saved.
Configure Static DHCP Bindings

You can view, add, and remove static bindings in the DHCP snooping bindings database and to view or clear the dynamic bindings in the bindings table.

**To view, add, and remove static DHCP bindings:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.

   The System Information page displays.

5. Select System > Services > DHCP Snooping > Binding Configuration.

6. From the Interface menu, select the interface on which the DHCP client is authorized.

7. In the MAC Address field, specify the MAC address for the binding to be added.
   
   This is the key to the binding database.

8. From the VLAN ID menu, select the ID of the VLAN that the client is authorized to use.

9. In the IP Address field, specify the IP address of the client.

10. Click the Add button.
   
    The DHCP snooping binding entry is added to the database.

11. To refresh the page with the latest information about the switch, click the Refresh button.

12. To deletes all DHCP snooping binding entries, click the Clear button.
The Dynamic Binding Configuration table shows information about the DHCP bindings that were learned on each interface on which DHCP snooping is enabled. The following table describes the dynamic bindings information.

**Table 25. DHCP Dynamic Configuration information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface on which the DHCP client message was received.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address associated with the DHCP client that sent the message. This is the key to the binding database.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID of the client interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address assigned to the client by the DHCP server.</td>
</tr>
<tr>
<td>Lease Time</td>
<td>The remaining IP address lease time for the client.</td>
</tr>
</tbody>
</table>

**Configure DHCP Snooping Persistent Settings**

You can configure the persistent location of the DHCP snooping bindings database. The bindings database can be stored locally on the device or on a remote system somewhere else in the network. The device must be able to reach the IP address of the remote system to send bindings to a remote database.

**To configure DHCP snooping persistent settings:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.
   
   The System Information page displays.

5. Select **System > Services > DHCP Snooping > Persistent Configuration**.
   
   The Persistent Configuration page displays.

6. Specify where the DHCP snooping bindings database is located.
   
   • **Local**. The binding table is stored locally on the switch.
   
   • **Remote**. The binding table is stored on a remote TFTP server.
If the database is stored on a remote server, specify the following information:

- **Remote IP Address.** Specify the IP address of the TFTP server.
- **Remote File Name.** Specify the file name of the DHCP snooping bindings database in which the bindings are stored.

7. In the **Write Delay** field, specify the time that the switch must wait after writing binding information to persistent storage.

   The delay allows the switch to collect as many entries as possible (new and removed) before writing them to the persistent file. You can specify from 15 to 86400 seconds. By default, the delay is 300 seconds.

8. Click the **Apply** button.

   Your settings are saved.

---

### View or Clear DHCP Snooping Statistics

You can view and clear per-interface statistics about the DHCP messages filtered by the DHCP snooping feature on untrusted interfaces.

**To view or clear the DHCP snooping statistics:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.

   The login window opens.

4. Enter the switch’s password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **System > Services > DHCP Snooping > Statistics**.

   The DHCP Snooping Statistics page displays.

6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:

   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.

7. To refresh the page with the latest information about the switch, click the **Refresh** button.
8. To clear all DHCP snooping statistics, click the **Clear** button.
The following table describes the DHCP snooping statistics.

**Table 26. DHCP Snooping Statistics information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface associated with the rest of the data in the row.</td>
</tr>
<tr>
<td>MAC Verify Failures</td>
<td>The number of DHCP messages that were dropped because the source MAC address and client hardware address did not match. MAC address verification is performed only if it is globally enabled.</td>
</tr>
<tr>
<td>Client Ifc Mismatch</td>
<td>The number of packets that were dropped by DHCP snooping because the interface and VLAN on which the packet was received do not match the client’s interface and VLAN information stored in the binding database.</td>
</tr>
<tr>
<td>DHCP Server Msgs</td>
<td>The number of DHCP server messages (such as DHCPOFFER, DHCPACK, DHCPNAK, and DHCPRELEASEQUERY messages) that were dropped on an untrusted port.</td>
</tr>
</tbody>
</table>

**Set Up PoE Timer Schedules**

The switch lets you define multiple timer schedules (each with a unique name) that you can use for PoE power delivery to attached PDs.

After you create a timer schedule, you can associate it with one or more PoE ports (see **Configure the PoE Port Settings on page 74**). You can use a separate timer schedule for each PoE port.

After you associate a timer schedule with a PoE port, the start date and time force the PoE port to **stop** delivering power and the stop date and time enable the PoE port to **start** delivering power.

You can create absolute timer schedules, which apply to specific dates and times, and you can create recurring timer schedules. For each timer schedule, you can add multiple entries that apply to the selected timer schedule only.

**Create a PoE Timer Schedule**

The maximum number of timer schedules that you can add is 100.

**To create a PoE timer schedule:**

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.

   The System Information page displays.

5. Select System > Timer Schedule > Basic > Global Configuration.

   The Timer Schedule Name page displays.

6. In the Timer Schedule Name field, specify the name for a timer schedule.

7. Click the Add button.

   The timer schedule is added to the table on the Timer Schedule Name page and is assigned an ID.

Specify the Settings for an Absolute PoE Timer Schedule

An absolute timer schedule applies to specific dates and times. The schedule is executed once only.

To specify the settings for a PoE timer schedule that uses specific dates and times:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.

   The System Information page displays.

5. Select System > Timer Schedule > Advanced > Timer Schedule Configuration.

   The Timer Schedule Configuration page displays.

6. In the Timer Schedule Selection section, make your selections from the following menus:
   a. Timer Schedule Name. Select the name of the timer schedule that you want to configure.
You can select only names of schedules that you created (see Create a PoE Timer Schedule on page 106).

b. **Timer Schedule Type.** Select Absolute.

The fields in the Timer Schedule Configuration section might adjust to let you configure a timer schedule for specific dates and times.

c. **Timer Schedule Entry.** To add a new entry, select new.

Selecting an existing entry lets you make changes to that entry.

7. In the Timer Schedule Configuration section, specify the times and dates:

a. In the **Time Start** field, enter the time of day in the HH:MM format to specify when the timer schedule must start.

b. In the **Time End** field, enter the time of day in the HH:MM format to specify when the timer schedule must stop.

c. Next to the **Date Start** field, click the calendar icon and use the menus in the pop-up window to enter the date in the DD-Mon-YYY format to specify when the timer schedule must start.

d. Next to the **Date End** field, click the calendar icon and use the menus in the pop-up window to enter the date in the DD-Mon-YYY format to specify when the timer schedule must stop.

8. Click the **Add** button.

The entry for the timer schedule is added.

Specify the Settings for a Recurring PoE Timer Schedule

A recurring schedule allows you to set up a single schedule that starts at a particular date and that recurs either with a specific end date or indefinitely.

For a single recurring PoE timer schedule, you can add a daily, weekly, and monthly schedule configuration. That is, these schedule configurations are not mutually exclusive but complement each other.

**To specify the settings for a PoE timer schedule that uses a recurring pattern:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the **Password** field.
The default password is **password**.

The System Information page displays.

5. Select **System > Timer Schedule > Advanced > Timer Schedule Configuration**.

The Timer Schedule Configuration page displays.

6. In the Timer Schedule Selection section, make your selections from the following menus:
   a. **Timer Schedule Name.** Select the name of the timer schedule that you want to configure.
      You can select only names of schedules that you created (see Create a PoE Timer Schedule on page 106).
   
   b. **Timer Schedule Type.** Select **Periodic**.
      The fields in the Timer Schedule Configuration section might adjust to let you configure a timer schedule with a recurrence pattern.
   
   c. **Timer Schedule Entry.** To add a new entry, select **new**.
      Selecting an existing entry lets you make changes to that entry.

7. In the Timer Schedule Configuration section, specify the recurrence pattern:
   a. In the **Time Start** field, enter the time of day in the HH:MM format to specify when the timer schedule must start.
   
   b. In the **Time End** field, enter the time of day in the HH:MM format to specify when the timer schedule must stop.
   
   c. Next to the **Date Start** field, click the calendar icon and use the menus in the pop-up window to enter the date in the DD-Mon-YYY format to specify when the timer schedule must start.
   
   d. Either select the **No End Date** radio button or select the **End Date** radio button, and next to the **End Date** field, click the calendar icon and use the menus in the pop-up window to enter the date in the DD-Mon-YYY format to specify when the timer schedule must stop.
   
   e. From the **Recurrence Pattern** menu, select the pattern:
      • **Daily.** The timer schedule works with daily recurrence. The fields adjust.
      
      Either select the **Every Weekday** radio button to let the schedule operate from Monday through Friday or select the **Every Day(s)** radio button and enter a number from 0 to 255 in the field.
      
      In the latter case, the schedule is triggered every specified number of days. If the number of days is not specified, or if you enter 0, then the schedule is triggered only once.
      
      • **Weekly.** The timer schedule works with weekly recurrence. The fields adjust.
      
      In the **Every Week(s)** field, enter a number from 0 to 255 to specify that the schedule must be triggered every specified number of weeks. If the number of weeks is not specified, or if you enter 0, then the schedule is triggered only once.
Select a single **Week Day** check box, multiple check boxes, or all check boxes to specify the day or days of the week that the schedule must operate.

- **Monthly.** The timer schedule works with monthly recurrence. The fields adjust.
  
  In the **Day** field, enter a number from 1 to 31 to specify the day of the month when the schedule must be triggered.
  
  In the **Every Month(s)** field, enter a number from 0 to 255 to specify that the schedule must be triggered every specified number of months. If the number of months is not specified, or if you enter 0, then the schedule is triggered only once.

8. Click the **Add** button.

The entry for the timer schedule is added.

**Change the Settings for a Recurring PoE Timer Schedule Entry**

You can change the settings for an existing recurring PoE timer schedule entry. (You cannot do this for an existing absolute PoE timer schedule.)

**To change the settings for an existing recurring PoE timer schedule entry:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.

   The System Information page displays.

5. Select **System > Timer Schedule > Advanced > Timer Schedule Configuration**.
   
   The Timer Schedule Configuration page displays.

6. From the **Timer Schedule Name** menu, select the schedule name.

7. From the **Timer Schedule Type** menu, select the schedule type.

8. From the **Timer Schedule Entry** menu, select the schedule entry.

9. Make the changes to the schedule entry.

   For more information, see Specify the Settings for a Recurring PoE Timer Schedule on page 108.
10. Click the **Apply** button.
    Your settings are saved.

Delete a PoE Timer Schedule Entry

You can delete a PoE timer schedule entry that you no longer need.

**To delete a PoE timer schedule entry:**

1. Connect your computer to the same network as the switch.
    You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
    If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address on page 12**.
    The login window opens.

4. Enter the switch’s password in the **Password** field.
    The default password is **password**.
    The System Information page displays.

5. Select **System > Timer Schedule > Advanced > Timer Schedule Configuration**.
    The Timer Schedule Configuration page displays.

6. From the **Timer Schedule Name** menu, select the schedule name.

7. From the **Timer Schedule Type** menu, select the schedule type.

8. From the **Timer Schedule Entry** menu, select the schedule entry.

9. Click the **Delete** button.
    The entry is deleted.

Delete a PoE Timer Schedule

You can delete a PoE timer schedule that you no longer need. All entries that are part of the PoE timer schedule are also deleted.

**To delete a PoE timer schedule:**

1. Connect your computer to the same network as the switch.
    You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch's password in the Password field.
   The default password is password.
   The System Information page displays.
5. Select System > Timer Schedule > Basic > Global Configuration.
   The Timer Schedule Name page displays.
6. Select the check box for the schedule that you want to delete.
7. Click the Delete button.
   The schedule is deleted.
This chapter contains the following sections:

- Configure the Port Settings and Maximum Frame Size
- Configure Link Aggregation Groups
- Configure VLANs
- Configure Auto-VoIP
- Configure Spanning Tree Protocol
- Configure Multicast
- View, Search, and Manage the MAC Address Table
- Configure Layer 2 Loop Protection
Configure the Port Settings and Maximum Frame Size

You can view, configure, and monitor the physical port information for the ports (that is, the physical interfaces) on the switch.

To configure the port settings and maximum frame size:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Switching > Ports > Port Configuration.

6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   • 1 (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   • LAG. Only LAGs are displayed.
   • All. Both physical interfaces and LAGs are displayed.

7. Select one or more interfaces by taking one of the following actions:
   • To configure a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   • To configure multiple interfaces with the same settings, select the check box associated with each interface.
• To configure all interfaces with the same settings, select the check box in the heading row.

8. In the **Description** field, enter the description string to be attached to a port.
   The string can be up to 64 characters in length.

9. From the **Admin Mode** menu, select **Enable** or **Disable**.
   This selection specifies the administrative mode for port control. You must select **Enable** in order for the port to participate in the network. The default is **Enable**.

10. From the **Autonegotiation** menu, select **Enable** or **Disable**.
    This selection specifies the autonegotiation mode for the port. The default is **Enable**.

    **Note:** After you change the autonegotiation mode, the switch might be inaccessible for a number of seconds while the new settings take effect.

11. In the **Speed** field, specify the speed value for the selected port.
    Possible field values are as follows:
    - **Auto**. All supported speeds.
    - **10**. 10 Mbits/second
    - **100**. 100 Mbits/second
    
    The delimiter characters for setting different speed values are a comma (,), a period (.) and a space ( ). For you to set the autonegotiation speed, the autonegotiation mode must be set to **Enable**. The default is **Auto**.

    **Note:** After you change the speed value, the switch might be inaccessible for a number of seconds while the new settings take effect.

12. From the **Duplex Mode** menu, select the duplex mode for the selected port.
    The options are as follows:
    - **Half**. Indicates that the interface supports transmission between the devices in only one direction at a time.
    - **Full**. Indicates that the interface supports transmission between the devices in both directions simultaneously.
    - **Auto**. Indicates that speed is set by the auto-negotiation process.
    
    The default is **Auto**.

    **Note:** After you change the duplex mode, the switch might be inaccessible for a number of seconds while the new settings take effect.

13. From the **Link Trap** menu, select whether or not to send a trap when the link status changes.
    By default, the switch sends a link trap.
14. In the Frame Size (1500 to 9198) field, specify the maximum Ethernet frame size that each interface can support.

The frame size includes the Ethernet header, CRC, and payload. The range is 1500 to 9198. The default maximum frame size is 1500.

15. From the Flow Control menu, select the configuration for IEEE 802.3 flow control.
   - Disable. If the port buffers become full, the switch does not send pause frames, and data loss could occur. This is the default setting.
   - Symmetric. If the port buffers become full, the switch sends pause frames to stop traffic.

   Flow control helps to prevent data loss when the port cannot keep up with the number of frames being switched. When you enable flow control, the switch can send a pause frame to stop traffic on the port if the amount of memory used by the packets on the port exceeds a preconfigured threshold and responds to pause requests from partner devices. The paused port does not forward packets for the time that is specified in the pause frame. When the pause frame time elapses, or the utilization returns to a specified low threshold, the switch enables the port to again transmit frames. The switch also honors incoming pause frames by temporarily halting transmission.

   - Asymmetric. If the port buffers become full, the switch does not send pause frames, and data loss could occur. However, the switch does honor incoming pause frames by temporarily halting transmission.

   Note: For LAG interfaces, flow control mode is displayed as a blank field because flow control is not applicable.

16. Click the Apply button.

   Your settings are saved.

The following table describes the nonconfigurable data that is displayed.

Table 27. Port Configuration information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Type</td>
<td>For normal ports this field is blank. Otherwise, the options are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Mirrored. The port is a mirrored port on which all the traffic is copied to the probe port.</td>
</tr>
<tr>
<td></td>
<td>• Probe. Use the port to monitor a mirrored port.</td>
</tr>
<tr>
<td></td>
<td>• Trunk Member. The port is a member of a link aggregation trunk. Look at the LAG pages for more information.</td>
</tr>
<tr>
<td>Physical Status</td>
<td>The port speed and duplex mode.</td>
</tr>
<tr>
<td>Link Status</td>
<td>Indicates whether the link is up or down.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The physical address of the specified interface.</td>
</tr>
</tbody>
</table>
Configure 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. By default, the LAG becomes a member of the default management VLAN (that is, VLAN 1).

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.

The switch supports static LAGs. When a port is added to a LAG as a static member, the port neither transmits nor receives LACPDUs.

The switch supports eight LAGs with a maximum of eight port members in each LAG.

Configure LAG Settings

You can 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 configure LAG settings:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
The System Information page displays.

5. **Select Switching > LAG > Basic > LAG Configuration.**

![Image of LAG Configuration table]

6. **In the LAG Name field, enter a name for the LAG.**
   You can enter any string of up to 15 alphanumeric characters.

7. **In the Description field, enter the description string to be attached to the LAG.**
   The description can be up to 64 characters in length.

8. **From the Admin Mode menu, select Enable or Disable.**
   When the LAG is disabled, no traffic flows and LACPDU s are dropped, but the links that form the LAG are not released. The default is Enable.

9. **From the Hash Mode menu, select the load-balancing mode for a port channel (LAG):**
   - **1 Src MAC, VLAN, EType, incoming port.** This mode uses the source MAC address, VLAN, EtherType, and incoming port that are associated with the packet.
   - **2 Dest MAC, VLAN, EType, incoming port.** This mode uses the destination MAC address, VLAN, EtherType, and incoming port that are associated with the packet.
   - **3 Src/Dest MAC, VLAN, EType, incoming port.** This mode uses the source and destination MAC addresses, VLAN, EtherType, and incoming port that are associated with the packet. This is the default mode.
   - **4 Src IP and Src TCP/UDP Port Fields.** This mode uses the source IP address and source TCP or UDP port value that are associated with the packet.
   - **5 Dest IP and Dest TCP/UDP Port Fields.** This mode uses the destination IP address and destination TCP or UDP port value that are associated with the packet.
   - **6 Src/Dest IP and TCP/UDP Port Fields.** This mode uses the source and destination IP addresses and source and destination TCP or UDP port values that are associated with the packet.

   **Note:** The switch balances traffic on a port channel (LAG) by selecting one of the links in the channel over which packets must be transmitted. The switch selects the link by creating a binary pattern from selected fields in a packet and associating that pattern with a particular link.

10. **From the STP Mode menu, select the Spanning Tree Protocol (STP) administrative mode associated with the LAG:**
   - **Disable.** Spanning tree is disabled for this LAG.
• **Enable.** Spanning tree is enabled for this LAG. Enable is the default.

**11.** From the Link Trap menu, select **Enable** or **Disable** to specify whether to send a trap when the link status changes.

The default is Enable, which causes the trap to be sent.

**12.** From the LAG Type menu, select **Static** or **LACP**:

- **Static.** Disables Link Aggregation Control Protocol (LACP) on the selected LAG. The LAG is configured manually. The default is Static.
- **LACP.** Enables LACP on the selected LAG. The LAG is configured automatically.

**13.** Click the **Apply** button.

Your settings are saved.

The following table describes the nonconfigurable information displayed on the page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAG ID</td>
<td>The identification of the LAG (l1–l8).</td>
</tr>
<tr>
<td>Active Ports</td>
<td>Indicates the ports that are actively participating in the port channel.</td>
</tr>
<tr>
<td>LAG State</td>
<td>Indicates whether the link is up or detached.</td>
</tr>
</tbody>
</table>

**Configure LAG Membership**

You can 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 a single link.

**To configure LAG membership:**

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address on page 12](#).

   The login window opens.

4. Enter the switch’s password in the **Password** field.
   - The default password is **password**.

   The System Information page displays.

5. Select **Switching > LAG > Basic > LAG Membership**.
The previous figure shows the LAG Membership page for models GS324T and GS324TP.

6. From the **LAG ID** menu, select the LAG ID.
7. In the **LAG Name** field, enter the name to be assigned to the LAG.
   You can enter any string of up to 15 alphanumeric characters. You can also use the default name.
8. In the Ports table, click each port that you want to include as a member of the selected LAG.
   A selected port is displayed by a check mark.
9. Click the **Apply** button.
   Your settings are saved.

**Set the LACP System Priority**

You can set the LACP system priority that applies to all LAGs on the switch.

**To configure LACP:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch's password in the **Password** field.
   The default password is **password**.
   The System Information page displays.
5. Select **Switching > LAG > Advanced > LACP Configuration**.
6. In the **LACP System Priority** field, specify the switch’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 setting globally by specifying a priority from 1 to 65535. The default value is 32768.

7. Click the **Apply** button.

   Your settings are saved.

---

**Set the LACP Port Priority Settings**

The LACP port configuration page is used to configure the LACP priority value for the selected port and the administrative LACP time-out value.

**To configure LACP port priority settings:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.

   The login window opens.

4. Enter the switch’s password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > LAG > Advanced > LACP Port Configuration**.
6. Select one or more interfaces by taking one of the following actions:
   • To configure a single interface, select the check box associated with the interface, or type the interface number in the Go To Interface field and click the Go button.
   • To configure multiple interfaces with the same settings, select the check box associated with each interface.
   • To configure all interfaces with the same settings, select the check box in the heading row.

7. In the LACP Priority field, specify the LACP priority value for the selected interfaces.
   This value specifies the interface'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. The range is 1 to 65535. The default value is 128.

8. In the Timeout field, configure the administrative LACP time-out value:
   • Long. Specifies a long time-out value.
   • Short. Specifies a short time-out value.

9. Click the Apply button.
   Your settings are saved.

Configure 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 is assigned 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 can omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet can either reject it or insert a tag using its default VLAN ID. A port can handle traffic for more than one VLAN, but it can support only one default VLAN ID.
You can define VLAN groups stored in the VLAN membership table. The switch supports up to 256 VLANs.

The following VLANs are preconfigured on the switch and you cannot delete them:

- **VLAN 1.** The default VLAN of which all ports are untagged members.
- **VLAN 4089.** The Auto-Video VLAN. By default, this VLAN does not include any members but you can manually add members.

### Configure VLAN Settings

You can configure the various VLAN settings.

#### Add a VLAN

**To add a VLAN:**

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.
   - The login window opens.
4. Enter the switch’s password in the **Password** field.
   - The default password is **password**.
   - The System Information page displays.
5. Select **Switching > VLAN > Basic > VLAN Configuration**.

![VLAN Configuration](image)

6. In the **VLAN ID** field, specify the VLAN identifier for the new VLAN.
   - The range of the VLAN ID can be from 2 to 4093, excluding 4089. (The default VLANs are 1 and 4089).
7. In the **VLAN Name** field, specify a name for the VLAN.
The VLAN name can be up to 32 alphanumeric characters long, including blanks. You cannot change the names of the default VLANs (that is, the VLANs with ID 1 and 4089).

8. The **VLAN Type** field displays the type of the VLAN that you are configuring.
   You cannot change the type of the default VLANs (that is, the VLANs with ID 1 and 4089). When you create a VLAN, its type is always Static. A VLAN that is dynamically created initially uses a type of Dynamic but you can manually change its type to Static.

9. Click the **Add** button.
   The VLAN is added to the switch.

**Delete a VLAN**

**To delete a VLAN from the switch:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **Switching > VLAN > Basic > VLAN Configuration**.
   The VLAN Configuration page displays.

6. In the **VLAN ID** field, specify the VLAN identifier.
   The range of the VLAN ID can be from 2 to 4093, excluding 4089.

   **Note:** You cannot delete VLANs 1 and 4089, all of which are predefined.

7. Click the **Delete** button.
   The VLAN is removed.
Reset the VLAN Configuration on the Switch to the Default Settings

If you reset the VLAN configuration on the switch to the default settings, all VLANs that you added are deleted. (The predefined VLANs are not deleted).

The VLAN default values are as follows:

- All ports are assigned to the default VLAN of 1.
- All ports are configured with a PVID of 1.
- All ports are configured to an Acceptable Frame Types value of Admit All Frames.
- All ports are configured with ingress filtering disabled.
- All ports are configured to transmit only untagged frames.
- All dynamic entries are cleared.

To reset the VLAN configuration on the switch to the default settings:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
5. Select Switching > VLAN > Basic > VLAN Configuration.
   You can also select Switching > VLAN > Advanced > VLAN Configuration.
   The VLAN Configuration page displays.
6. Select the Reset Configuration check box.
7. Click the Apply button.
   Your settings are saved. Except for the predefined default VLANs, all VLANs are deleted.

Configure VLAN Membership

To configure VLAN membership:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch's password in the Password field.
   The default password is password.
   The System Information page displays.
5. Select Switching > VLAN > Advanced > VLAN Membership.

The previous figure shows the LAG Membership page for models GS324T and GS324TP.

6. In the VLAN ID menu, select the VLAN ID.
   You can select a VLAN that is predefined or that you added (see Add a VLAN on page 123).
7. In the Group Operation menu, select one of the following options, which applies to all ports in the VLAN:
   • Untag All. For all ports and LAGs that are members of the VLAN, tags are removed from all egress packets.
   • Tag All. For all ports and LAGs that are members of the VLAN, all egress packets are tagged.
   • Remove All. All ports and LAGs are removed from the VLAN.
8. In the Ports table, click each port once, twice, or three times to configure one of the following modes or reset the port to the default mode:
   • T (Tagged). Selects the port as a tagged port in the VLAN. All frames transmitted on the port are tagged for this VLAN.
• **U (Untagged).** Selects the port as an untagged port in the VLAN. All frames transmitted on the port are untagged for this VLAN.

• **Blank.** The port is excluded from the VLAN.

By default, the selection is blank and none of the ports are a member of the VLAN. (VLAN 1 is an exception. By default, all ports are untagged members of VLAN 1.)

9. In the LAG table, click each LAG once, twice, or three times to configure one of the following modes or reset the LAG to the default mode:

• **T (Tagged).** Selects the LAG as a tagged LAG in the VLAN. All frames transmitted on the LAG are tagged for this VLAN.

• **U (Untagged).** Selects the LAG as an untagged LAG in the VLAN. All frames transmitted on the LAG are untagged for this VLAN.

• **Blank.** The LAG is excluded from the VLAN.

By default, the selection is blank and none of the LAGs are a member of the VLAN. (VLAN 1 is an exception. By default, all LAGs are untagged members of VLAN 1.)

10. Click the **Apply** button.

Your settings are saved.

The following table describes the nonconfigurable information displayed on the page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Name</td>
<td>The name for the VLAN that you selected. It can be up to 32 alphanumeric characters long, including blanks. The names for the following VLANs are predefined:</td>
</tr>
<tr>
<td></td>
<td>• <strong>VLAN 1.</strong> Default.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VLAN 4089.</strong> Auto-Video.</td>
</tr>
<tr>
<td>VLAN Type</td>
<td>The type of the VLAN you selected:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default</strong> (VLAN ID = 1). Always present.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Static.</strong> A VLAN that you configured.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dynamic.</strong> A dynamically created VLAN.</td>
</tr>
</tbody>
</table>

**View the VLAN Status**

You can view the status of all currently configured VLANs.

**To view the VLAN status:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

The login window opens.

4. Enter the switch’s password in the Password field. The default password is password.

The System Information page displays.

5. Select Switching > VLAN > Advanced > VLAN Status.

The previous figure includes one manually configured VLAN (VLAN ID 33).

**Note:** A nonoperational LAG is excluded from the VLAN Status page. Only when the member LAG is operationally up, is the LAG port displayed on the VLAN Status page. For example, LAG1 (ch1) is not listed in the Member Ports column for VLAN1 because LAG1 is not operationally up.

The following table describes the nonconfigurable information displayed on the page.

**Table 30. VLAN status**

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>The VLAN identifier (VID) of the VLAN. The range of the VLAN ID is from 1 to 4093.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>The name of the VLAN.</td>
</tr>
</tbody>
</table>
| VLAN Type     | The VLAN type:  
|               | • Default (VLAN ID = 1). Always present.                                    |
|               | • Auto-Video (VLAN ID = 4089). Always present.                              |
|               | • Static. A VLAN that you configured.                                       |
|               | • Dynamic. A dynamically created VLAN.                                       |
| Member Ports  | The ports, LAGs, or both that are included in the VLAN.                     |
Configure Port PVID Settings

You can assign a port VLAN ID (PVID) to an interface. The following requirements apply to a PVID:

• By default, the PVID for each port is 1.
• If you do not specify another value, the default VLAN PVID is used.
• To change the port’s default PVID, you must first create a VLAN that includes the port as a member (see Configure VLAN Membership on page 125).

Note: If you remove the management VLAN (by default, VLAN 1) as the PVID from all ports, you can no longer access the switch over the local browser interface. In that situation, you must reset the switch to factory default settings. However, the PVID Lockout Warning feature prevents you from removing the management VLAN as the PVID from all ports. This feature is enabled by default and you cannot disable it.

To configure PVID settings:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Switching > VLAN > Advanced > Port PVID Configuration.
The previous figure does not show all columns on the page.

6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   • 1 (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   • LAG. Only LAGs are displayed.
   • All. Both physical interfaces and LAGs are displayed.

7. Select one or more interfaces by taking one of the following actions:
   • To configure a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   • To configure multiple interfaces with the same settings, select the check box associated with each interface.
   • To configure all interfaces with the same settings, select the check box in the heading row.

8. In the PVID field, specify the VLAN ID to assign to untagged or priority-tagged frames received on the port.
   The default is 1. The range is from 2 to 4093, excluding 4089.

9. In the VLAN Member field, specify the VLAN ID or list of VLANs of a member port.
   VLAN IDs range from 2 to 4093, excluding 4089. The default is 1. Use a hyphen (-) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.

10. In the VLAN Tag field, specify the VLAN ID or list of VLANs of a tagged port.
    VLAN IDs range from 2 to 4093, excluding 4089. Use a hyphen (-) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted. You can specify port tagging for the VLAN only if the port that you want to add as a tagged port is also member of the VLAN. To reset the VLAN tag configuration to the defaults, use the None keyword.

11. From the Acceptable Frame menu, specify one of the following types of frames that can be received on the port:
    • Admit All. Untagged frames or priority-tagged frames that are received on the port are accepted and assigned the value of the port VLAN ID for the port. This is the default selection.
    • VLAN Only. Untagged frames or priority-tagged frames that are received on the port are discarded.
    • Admit Untagged Only. Untagged frames that are received on the port are accepted.
    With the Admit All and VLAN Only selections, VLAN-tagged frames are forwarded in accordance to the 802.1Q VLAN specification.

12. From the Ingress Filtering menu, select one of the following options:
    • Enable. The frame is discarded if the port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is 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 802.1Q VLAN bridge specification. The default is Disable.

13. In the **Port Priority** field, specify the default 802.1p priority assigned to untagged packets arriving at the port.

You can enter a number from 0 to 7.

14. Click the **Apply** button.

Your settings are saved.

The following table describes the nonconfigurable fields.

**Table 31. Nonconfigurable fields on the PVID Configuration page**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Ingress Filtering</td>
<td>Indicates whether ingress filtering is enabled for the interface.</td>
</tr>
<tr>
<td>Untagged VLANs</td>
<td>The number of untagged VLANs for the interface.</td>
</tr>
<tr>
<td>Tagged VLANs</td>
<td>The number of tagged VLANs for the interface.</td>
</tr>
<tr>
<td>Forbidden VLANs</td>
<td>The number of forbidden VLANs for the interface.</td>
</tr>
<tr>
<td>Dynamic VLANs</td>
<td>The number of dynamically added VLANs for the interface.</td>
</tr>
</tbody>
</table>

**Configure a MAC-Based VLAN**

The MAC-Based VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the source MAC address of the packet.

You define a MAC-to-VLAN mapping by configuring an entry in the MAC-to-VLAN table. An entry is specified through a source MAC address and a VLAN ID. The MAC-to-VLAN configurations are shared across all ports of the switch (that is, a system-wide table exists with MAC address–to–VLAN ID mappings).

When untagged or priority-tagged packets arrive at the switch and entries exist in the MAC-to-VLAN table, the source MAC address of the packet is looked up. If an entry is found, the corresponding VLAN ID is assigned to the packet. If the packet is already priority-tagged, it maintains this value. Otherwise, the priority is set to zero. The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues. Otherwise, the packet is dropped. This implies that you can configure a MAC address mapping to a VLAN that you did not yet create on the switch.
Add a MAC-Based VLAN

**To add a MAC-based VLAN:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.
   
   The System Information page displays.

5. Select **Switching** > **VLAN** > **Advanced** > **MAC Based VLAN**.

6. In the **MAC Address** field, enter a MAC address to be bound to a VLAN ID.
   
   This field is configurable only when a MAC-based VLAN is created.

7. In the **VLAN ID** field, specify a VLAN ID in the range from 2 to 4093, excluding 4089.

8. Click the **Add** button.
   
   The MAC address is added to the VLAN mapping.

Delete a MAC Address From VLAN Mapping

**To delete a MAC address from VLAN mapping:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.
4. Enter the switch’s password in the **Password** field.  
The default password is **password**.  
The System Information page displays.

5. Select **Switching > VLAN > Advanced > MAC Based VLAN**.  
The MAC Based VLAN Configuration page displays.

6. In the **MAC Address** field, enter a MAC address.  
   This field is configurable only when a MAC-based VLAN exists.

7. In the **VLAN ID** field, specify a VLAN ID in the range from 2 to 4093, excluding 4089.
8. Click the **Delete** button.  
The MAC address is removed from the VLAN mapping.

### Configure Protocol-Based VLAN Groups

You can use a protocol-based VLAN to define filtering criteria for untagged packets. By default, if you do not configure any port-based (IEEE 802.1Q) or protocol-based VLANs, untagged packets are assigned to VLAN 1. You can override this behavior by defining either port-based VLANs or protocol-based VLANs, or both. Tagged packets are always handled according to the IEEE 802.1Q standard and are not included in protocol-based VLANs.

If you assign a port to a protocol-based VLAN for a specific protocol, untagged frames that arrive on that port for that protocol are assigned the protocol-based VLAN ID. Untagged frames that arrive on the port for other protocols are assigned the port VLAN ID, either the default PVID (1) or a PVID you specifically assigned to the port (see **Configure Port PVID Settings** on page 129).

You define a protocol-based VLAN by creating a group. Each group forms a one-to-one relationship with a VLAN ID, can include one to three protocol definitions, and can include multiple ports. When you create a group, you specify a name and a group ID is assigned automatically.

**To configure a protocol-based VLAN group:**

1. Connect your computer to the same network as the switch.  
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.  
   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address** on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
The default password is `password`.

The System Information page displays.

5. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration**.

   ![Protocol Based VLAN Group Configuration](image)

6. In the **Group ID** field, enter a number to identify the group.
   
The number must be in the range from 1 to 128.

7. In the **Group Name** field, enter a name for the new group.
   
   You can enter up to 16 characters.

8. In the **Protocol** field, enter one or more protocols that must be associated with the group.
   
   You can enter keywords such as `arp`, `ip`, and `ipx`. Separate keywords with a comma. You can also enter hexadecimal or decimal values in the range from `0x0600` (1536) to `0xFFFF` (65535).

9. In the **VLAN ID** field, enter the VLAN ID.
   
   The ID can be any number in the range from 2 to 4093, excluding 4089. All the ports in the group assign this VLAN ID to untagged packets received for the protocols that you included in this group.

10. Click the **Add** button.

    The protocol-based VLAN group is added to the switch.

    The Ports field displays all the member ports that belong to the group.

---

### Configure Protocol-Based VLAN Group Membership

**To configure protocol-based VLAN group membership:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address on page 12](#).
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
The default password is **password**.

The System Information page displays.

5. **Select Switching > VLAN > Advanced > Protocol Based VLAN Group Membership.**

![Protocol Based VLAN Group Membership page](image)

The previous figure shows the Protocol Based VLAN Group Membership page for models GS324T and GS324TP.

6. **From the Group ID menu, select the protocol-based VLAN group ID.**

   The Group Name field shows the name that is associated with the group.

7. **In the Ports table and LAG table, click each port and LAG that you want to include in the protocol-based VLAN group.**

   A protocol-based VLAN group can include both port and LAGs. A selected port or LAG is displayed by a check mark.

8. **Click the Apply button**

    Your settings are saved.

9. **To display the current numbers in the selected protocol-based VLAN group, click the Current Members button.**

### Configure a Voice VLAN

You can configure the settings for a voice VLAN configuration.

**To configure a voice VLAN:**

1. **Connect your computer to the same network as the switch.**

    You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. **Launch a web browser.**
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Switching > VLAN > Advanced > Voice VLAN Configuration.

6. Select the Admin Mode Disable or Enable radio button.
   This selection specifies the administrative mode for the voice VLAN for the switch. The default is Disable.

7. Select the interface by taking one of the following actions:
   • To configure a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   • To configure multiple interfaces with the same settings, select the check box associated with each interface.
   • To configure all interfaces with the same settings, select the check box in the heading row.

8. From the Interface Mode menu, select the voice VLAN mode for selected interfaces:
   • Disable. This is the default value.
   • None. Allow the IP phone to use its own configuration to send untagged voice traffic.
   • VLAN ID. Configure the phone to send tagged voice traffic. You must enter the VLAN ID in the Value field (see the next step).
   • Dot1p. Configure voice VLAN 802.1p priority tagging for voice traffic. You must enter the dot1p value in the Value field (see the next step).
   • Untagged. Configure the phone to send untagged voice traffic.
9. In the **Value** field, enter the VLAN ID or dot1p value.
   This field is enabled only if you select **VLAN ID** or **Dot1p** from the **Interface Mode** menu.

10. In the **CoS Override Mode** field, select **Disable** or **Enable**.
    The default is **Disable**.

11. In the **Authentication Mode** field, select **Enable** or **Disable**.
    The default is **Enable**. When the authentication mode is enabled, voice traffic is allowed on an unauthorized voice VLAN port. When the authentication mode is disabled, devices are authorized through dot1x.

    **Note:** Authentication through dot1x is possible only if dot1x is enabled.

12. In the **DSCP Value** field, configure the Voice VLAN DSCP value for the port.
    The range is from 0 to 64. The default value is 0.

13. Click the **Apply** button.
    Your settings are saved.
    The **Operational State** field displays the operational status of the voice VLAN on an interface.

---

### Configure Auto-VoIP

Voice over Internet Protocol (VoIP) enables telephone calls over a data network. Because voice traffic is typically more time-sensitive than data traffic, the Auto-VoIP feature provides a classification for voice packets so that they can be prioritized above data packets, allowing the switch to provide better Quality of Service (QoS). With the Auto-VoIP feature, voice prioritization is provided based on call-control protocols (SIP, SCCP, or H.323) or OUI bits.

---

### Configure Protocol-Based Port Settings for VoIP

To prioritize time-sensitive voice traffic over data traffic, protocol-based Auto-VoIP checks for packets carrying the following VoIP protocols:

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

VoIP frames that are received on ports that for which the Auto-VoIP feature is enabled are marked with the specified CoS traffic class value.
To configure protocol-based port settings for VoIP:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch's password in the Password field.
   The default password is password.
   The System Information page displays.


6. From the Prioritization Type menu, select Traffic Class or Remark.
   This selection specifies the type of prioritization.

7. From the Class Value menu, specify the CoS class value to be reassigned for packets that the voice VLAN receives.

8. Click the Apply button.
   Your settings are saved.

9. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - 1 (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - LAG. Only LAGs are displayed.
   - All. Both physical interfaces and LAGs are displayed.
10. Select one or more interfaces by taking one of the following actions:
   • To configure a single interface, select the check box associated with the port, or type
     the port number in the Go To Interface field and click the Go button.
   • To configure multiple interfaces with the same settings, select the check box
     associated with each interface.
   • To configure all interfaces with the same settings, select the check box in the heading
     row.

11. From the Auto VoIP Mode menu, select Disable or Enable.
    Auto-VoIP is disabled by default.

12. Click the Apply button.
    Your settings are saved.
    The Operational Status field displays the current operational status of an interface.

Configure Auto-VoIP OUI-Based Properties

With Organizationally Unique Identifier (OUI)–based Auto-VoIP, voice prioritization is
provided based on OUI bits.

To configure Auto-VoIP OUI-based properties:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or
   connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP
   Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Switching > Auto-VoIP > OUI-based > Properties.
   The OUI-Based Properties page displays.

6. In the Auto-VoIP VLAN ID field, enter the VoIP VLAN ID of the switch.
   No default VLAN exists for Auto-VoIP, you must create a VLAN for Auto-VoIP.

7. From the OUI-based priority menu, select the OUI-based priority of the switch, from 0 to 7.
   The default value is 7.
8. Click the **Apply** button.
Your settings are saved.

Configure the OUI-Based Port Settings

You can configure the OUI port settings.

**To configure OUI-based port settings:**
1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.
4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.
   
   The System Information page displays.
5. Select **Switching > Auto-VoIP > OUI-based > Port Settings**.

![OUI Port Settings](image)

6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   
   • **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   
   • **LAG**. Only LAGs are displayed.
   
   • **All**. Both physical interfaces and LAGs are displayed.
7. Select one or more interfaces by taking one of the following actions:
   
   • To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
To configure multiple interfaces with the same settings, select the check box associated with each interface.

To configure all interfaces with the same settings, select the check box in the heading row.

8. From the **Auto VoIP Mode** menu, select **Disable** or **Enable**.

Auto-VoIP is disabled by default.

9. Click the **Apply** button.

Your settings are saved.

The Operational Status field displays the current operational status of an interface.

**Manage the OUI Table**

Device hardware manufacturers can include an OUI in a network adapter to help identify a hardware device. The OUI is a unique 24-bit number assigned by the IEEE registration authority. The switch comes preconfigured with the following OUIs that identify the IP phone manufacturer:

- 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
- 00:04:13: SNOM

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

**Configure the OUI Table**

**To configure the OUI Table:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Switching > Auto-VoIP > OUI-based > OUI Table.
   The OUI Table page displays.

6. In the Telephony OUI(s) field, specify the VoIP OUI prefix to be added in the format AA:BB:CC.
   You can configure up to 128 OUIs.

7. In the Description field, enter the description for the OUI.
   The maximum length of description is 32 characters.

8. Click the Add button.
   The telephony OUI entry is added.

Delete One or More OUI Prefixes From the OUI Table

To delete one or more OUI prefixes from the OUI table:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Switching > Auto-VoIP > OUI-based > OUI Table.
   The OUI Table page displays.

6. Select the check box next to each OUI prefix to be removed.

7. Click the Delete button.
   The telephony OUI entries are removed.
Display the Auto-VoIP Status

You can display the Auto-VoIP status.

To view the Auto-VoIP status:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Switching > Auto-VoIP > Auto-VoIP Status.
   The Auto-VoIP Status page displays.

6. To refresh the page with the latest information about the switch, click the Refresh button.

The following table describes the nonconfigurable Auto-VoIP status information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-VoIP VLAN ID</td>
<td>The Auto-VoIP VLAN ID.</td>
</tr>
<tr>
<td>Maximum Number of Voice Channels Supported</td>
<td>The maximum number of voice channels supported.</td>
</tr>
<tr>
<td>Number of Voice Channels Detected</td>
<td>The number of VoIP channels prioritized successfully.</td>
</tr>
</tbody>
</table>

Configure Spanning Tree Protocol

The Spanning Tree Protocol (STP) provides a tree topology for any arrangement of network devices. STP also provides one path between end stations on a network, eliminating loops. STP (also referred to as “classic” STP) provides a single path between end stations, avoiding and eliminating loops. For information about configuring the global STP settings for the switch, see Configure the STP Settings and View the STP Status on page 144.
The switch supports the following spanning tree versions:

- **CST**: Common STP. For information on configuring CST, see Configure and View the CST Settings on page 146 and Configure and View the CST Port Settings on page 148.

- **MSTP**: Multiple Spanning Tree Protocol (MSTP, also referred to as MST) supports multiple instances of spanning tree to efficiently channel VLAN traffic over different interfaces. For information on configuring MSTP, see Manage MST Settings on page 153 and Configure and View the Port Settings for an MST Instance on page 155.

- **RSTP**: Rapid STP. 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 the forwarding state). For information on viewing the RSTP state, see View Rapid STP Information on page 152.

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 with both RSTP and STP. It behaves in a way that is appropriate for STP and RSTP bridges. An MSTP bridge can be configured to behave entirely as an RSTP bridge or an STP bridge.

---

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

---

Configure the STP Settings and View the STP Status

You can configure the STP settings and view the STP status on the switch.

**To configure the STP settings and view the STP status:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
The default password is **password**.

The System Information page displays.

5. **Select Switching > STP > Basic > STP Configuration.**

6. Configure the following global settings for the switch:
   a. **Spanning Tree State.** Enable or disable the spanning tree operation on the switch.
      
      By default, spanning tree operation is disabled.
   b. **STP Operation Mode.** Specify the STP version for the switch.
      
      The options are **STP**, **RSTP**, and **MSTP**. The default is RSTP.
   c. **Configuration Name.** Specify a name to identify the STP, RSTP, or MSTP configuration.
      
      The name can be up to 32 alphanumeric characters.
   d. **Configuration Revision Level.** Specify an identifier to identify the STP, RSTP, or MSTP configuration.
      
      The values can be from 0 to 65535. The default value is 0.
   e. **Forward BPDU while STP Disabled.** Enable or disable the bridge protocol data unit (BPDU) flood.
      
      This setting specifies whether spanning tree BPDUs are forwarded while spanning tree is disabled on the switch.

7. **Click the Apply button.**

   Your settings are saved.

8. **To refresh the page with the latest information about the switch, click the Refresh button.**

The following table describes the nonconfigurable fields displayed on the page.

**Table 33. STP Configuration status**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Configuration Digest Key</td>
<td>The identifier used to identify the configuration currently being used.</td>
</tr>
<tr>
<td><strong>STP Status</strong></td>
<td></td>
</tr>
</tbody>
</table>
Configure and View the CST Settings

You can configure a Common Spanning Tree (CST) and Internal Spanning Tree on the switch.

To configure and view the CST settings:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
The default password is password.

The System Information page displays.

5. Select Switching > STP > Advanced > CST Configuration.

6. Specify the CST options:
   - **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. Specify the bridge priority value for the Common and Internal Spanning Tree (CST). The range is from 0 to 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 you set the priority to any value between 0 and 4095, the switch automatically sets the value to 0. The default value is 32768.
   - **Bridge Max Age (secs).** The bridge maximum age time for the Common and Internal Spanning Tree (CST), which indicates the time in seconds a bridge must wait before implementing a topological change. The range is from 6 to 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).** The bridge hello time for the Common and Internal Spanning Tree (CST), which indicates the time in seconds a root bridge must wait between configuration messages. The value is fixed at 2 seconds. The value must be less than or equal to (Bridge Max Age / 2) – 1. The default hello time value is 2.
   - **Bridge Forward Delay (secs).** The bridge forward delay time, which indicates the time in seconds a bridge must remain in a listening and learning state before forwarding packets. The value must be greater or equal to (Bridge Max Age / 2) + 1. The time range is from 4 seconds to 30 seconds. The default value is 15 seconds.
   - **Spanning Tree Maximum Hops.** The maximum number of bridge hops the information for a particular CST instance can travel before being discarded. The range is from 6 to 40. The default is 20 hops.

7. Click the Apply button.
   Your settings are saved.
8. To refresh the page with the latest information about the switch, click the Refresh button. The following table describes the MSTP Status information that is displayed.

Table 34. STP advanced CST configuration, MSTP status

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

Configure and View the CST Port Settings

You can configure a common spanning tree (CST) and internal spanning tree on a specific port on the switch.

A port can become diagnostically disabled (D-Disable) when DOT1S experiences a severe error condition. The most common cause is when the DOT1S software experiences BPDU flooding. The flooding criteria are such that DOT1S receives more than 15 BPDUs in a 3-second interval. The other causes for DOT1S D-Disable are very rare.

To configure and view the CST port settings:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Switching > STP > Advanced > CST Port Configuration.
6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   • 1 (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   • LAG. Only LAGs are displayed.
   • All. Both physical interfaces and LAGs are displayed.

7. Select one or more interfaces by taking one of the following actions:
   • To configure a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   • To configure multiple interfaces with the same settings, select the check box associated with each interface.
   • To configure all interfaces with the same settings, select the check box in the heading row.

8. From the STP Status menu, select the option to enable or disable the spanning tree administrative mode associated with the port or LAG.
   The option is Enable or Disable. The default value is Enable.

9. From the Fast Link menu, select whether the specified port is an edge port within the CST.
   The option is Enable or Disable. The default value is Disable.

10. From the BPDU Forwarding menu, configure BPDU forwarding.
    The option is Enable or Disable. The default value is Disable. When BPDU forwarding is enabled, the switch forwards the BPDU traffic arriving on the port when STP is disabled on the port.

11. From the Auto Edge menu, specify if the port is allowed to become an edge port if it does not detect BPDUs for some time.
    The option is Enable or Disable. The default value is Enable.

12. In the Path Cost field, set the path cost to a new value for the specified port in the common and internal spanning tree.
    Specify a value in the range from 0 to 200000000. The default is 0. When the path cost is set to 0, the value is updated with the external path cost from an incoming STP packet.

13. In the Priority field, specify the priority for a particular port within the CST.
The port priority is set in multiples of 16. For example if you attempt to set the priority to any value between 0 and 15, it is set to 0. If you try to set it to any value between 16 and \((2^4 - 1)\), it is set to 16, and so on. The range is 0 to 240. The default value is 128.

14. In the **External Port Path Cost** field, set the external path cost to a new value for the specified port in the spanning tree.
   The value range is 0 to 200000000. The default is 0.

15. Click the **Apply** button.
   Your settings are saved.

16. To refresh the page with the latest information about the switch, click the **Refresh** button.

The following table describes the nonconfigurable information displayed on the page.

**Table 35. CST port configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port State</td>
<td>The forwarding state of the port. The default is Disabled.</td>
</tr>
<tr>
<td>Port ID</td>
<td>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.</td>
</tr>
<tr>
<td>Hello Timer</td>
<td>The value of the setting for the CST. The default is 2 seconds.</td>
</tr>
</tbody>
</table>

**View the CST Port Status**

You can to display the common spanning tree (CST) and internal spanning tree for a specific port on the switch.

**To view the CST port status:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **Switching > STP > Advanced > CST Port Status**.
6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.

7. To refresh the page with the latest information about the switch, click the **Refresh** button.

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

**Table 36. CST port status**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The physical port or LAG that is 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 can be Root, Designated, Alternate, Backup, Master, or Disabled.</td>
</tr>
<tr>
<td>Designated Root</td>
<td>The root bridge for the CST. It is made up using the bridge priority and the base MAC address of the bridge.</td>
</tr>
<tr>
<td>Designated Cost</td>
<td>The path cost offered to the LAN by the designated port.</td>
</tr>
<tr>
<td>Designated Bridge</td>
<td>The identifier of the bridge with the designated port. It is made up using the bridge priority and the base MAC address of the bridge.</td>
</tr>
<tr>
<td>Designated Port</td>
<td>The 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.</td>
</tr>
<tr>
<td>Topology Change Acknowledge</td>
<td>Identifies whether the topology change acknowledgement flag is set for the next BPDU to be transmitted for the port. It is either True or False.</td>
</tr>
<tr>
<td>Edge port</td>
<td>Indicates whether the port is enabled as an edge port. It is either Enabled or Disabled.</td>
</tr>
</tbody>
</table>
View Rapid STP Information

You can view information about the Rapid Spanning Tree (RSTP) port status.

To view information about RSTP:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Switching > STP > Advanced > RSTP.

6. To refresh the page with the latest information about the switch, click the Refresh button.

The following table describes the Rapid STP Status information displayed on the page.

<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 can be Root, Designated, Alternate, Backup Master, or Disabled.</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 the port.</td>
</tr>
</tbody>
</table>
Manage MST Settings

You can configure a multiple spanning tree (MST) on the switch.

Configure an MST Instance

To configure an MST instance:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Switching > STP > Advanced > MST Configuration.

6. Configure the MST values:
   - **MST ID.** Specify the ID of the MST to create. The range is from 1 to 4094. This is visible only when the select option of the MST ID select box is selected.
   - **Priority.** 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 you set the priority to any value between 0 and 4095, the switch automatically sets the value to 0. The default value is 32768. The range is from 0 to 61440.
   - **VLAN ID.** The menu includes all VLANs that are configured on the switch. You can select VLANs that must be associated with the MST instance or clear VLANs that are already associated with the MST instance.

7. Click the Add button.
   The MST is added.
For each configured instance, the information described in the following table displays on the page.

**Table 38. MST configuration**

<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>Last TCN</td>
<td>The time in the format “day:hour:minute:second” since the topology of the selected MST instance last changed.</td>
</tr>
<tr>
<td>Topology Change Count</td>
<td>The number of times that the topology changed for the selected MST instance.</td>
</tr>
<tr>
<td>Topology Change</td>
<td>The value of the topology change settings for the switch, indicating if a topology change is in progress on any port assigned to the selected MST instance. It 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>The path cost to the designated root for this MST instance.</td>
</tr>
<tr>
<td>Root Port</td>
<td>The port to access the designated root for this MST instance.</td>
</tr>
</tbody>
</table>

**Modify an MST Instance**

**To modify an MST instance:**

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address on page 12**.
   - The login window opens.
4. Enter the switch's password in the **Password** field.
   - The default password is **password**.
   - The System Information page displays.
5. Select **Switching > STP > Advanced > MST Configuration**.
   - The MST Configuration page displays.
6. Select the check box next to the instance.
   - You can select multiple check boxes to apply the same setting to all selected ports.
7. Update the values.
8. Click the **Apply** button.
   Your settings are saved.

Delete an MST Instance

**To delete an MST instance:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address** on page 12.
   The login window opens.
4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.
5. Select **Switching > STP > Advanced > MST Configuration**.
   The MST Configuration page displays.
6. Select the check box for the instance.
7. Click the **Delete** button.
   The MST instance is removed.

Configure and View the Port Settings for an MST Instance

You can configure and display the Multiple Spanning Tree (MST) settings on a specific port on the switch.

A port can become diagnostically disabled (D-Disable) when DOT1S experiences a severe error condition. The most common cause is when the DOT1S software experiences BPDU flooding. The flooding criteria is such that DOT1S receives more than 15 BPDUs in a 3-second interval. The other causes for DOT1S D-Disable are extremely rare.

**To configure and view the port settings for an MST instance:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.

The System Information page displays.

5. Select Switching > STP > Advanced > MST Port Configuration.

The previous figure does not show all columns on the page.

If no MST instances are configured on the switch, the page displays a “No MSTs Available” message.

6. From the Select MST menu, select the MST instance.
   You can select only instances that you added to the switch (see Manage MST Settings on page 153).

7. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   • 1 (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   • LAG. Only LAGs are displayed.
   • All. Both physical interfaces and LAGs are displayed.

8. Select one or more interfaces by taking one of the following actions:
   • To configure a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   • To configure multiple interfaces with the same settings, select the check box associated with each interface.
   • To configure all interfaces with the same settings, select the check box in the heading row.

9. Configure the MST values for the selected interfaces:
   • 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. Specify a value in the range from 0 to 240.

- **Port Path Cost.** Set the path cost to a new value for the specified port in the selected MST instance. Specify a value in the range from 0 to 200000000.

10. Click the **Apply** button.

Your settings are saved.

11. To refresh the page with the latest information about the switch, click the **Refresh** button.

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>Operational Port Path Cost</td>
<td>Indicates the operational path cost that is based on the link speed of the port if the configured value for Port Path Cost is zero.</td>
</tr>
<tr>
<td>Auto Calculated Port Path Cost</td>
<td>Indicates whether the path cost is automatically calculated (Enabled) or not (Disabled). Path cost is calculated based on the link speed of the port if the configured value for Port Path Cost is zero.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.</td>
</tr>
<tr>
<td>Port Up Time Since Counters Last Cleared</td>
<td>The time since the counters were last cleared, displayed in days, hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Port Mode</td>
<td>The Spanning Tree Protocol administrative mode that is associated with the port or port channel. The option is Enable or Disable.</td>
</tr>
<tr>
<td>Port Forwarding State</td>
<td>The current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. The options are as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled.</strong> STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Blocking.</strong> The port is currently blocked. The port cannot forward traffic nor can it learn MAC addresses.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Listening.</strong> The port is currently in listening mode. The port cannot forward traffic 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. 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 learn new MAC addresses.</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 can be Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.</td>
</tr>
<tr>
<td>Designated Root</td>
<td>The root bridge for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.</td>
</tr>
</tbody>
</table>
You can view information about the number and type of bridge protocol data units (BPDUs) transmitted and received on each port.

To view the spanning tree statistics:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Switching > STP > Advanced > STP Statistics.

6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - 1 (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - LAG. Only LAGs are displayed.
- **All.** Both physical interfaces and LAGs are displayed.

7. To refresh the page with the latest information about the switch, click the **Refresh** button.

The following table describes the information available about the STP Statistics page.

**Table 40. STP Statistics**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The physical port or LAG on the switch.</td>
</tr>
<tr>
<td>STP BPDUs Received</td>
<td>The number of STP BPDUs received at the selected port.</td>
</tr>
<tr>
<td>STP BPDUs Transmitted</td>
<td>The number of STP BPDUs transmitted from the selected port.</td>
</tr>
<tr>
<td>RSTP BPDUs Received</td>
<td>The number of RSTP BPDUs received at the selected port.</td>
</tr>
<tr>
<td>RSTP BPDUs Transmitted</td>
<td>The number of RSTP BPDUs transmitted from the selected port.</td>
</tr>
<tr>
<td>MSTP BPDUs Received</td>
<td>The number of MSTP BPDUs received at the selected port.</td>
</tr>
<tr>
<td>MSTP BPDUs Transmitted</td>
<td>The number of MSTP BPDUs transmitted from the selected port.</td>
</tr>
</tbody>
</table>

**Configure Multicast**

Multicast IP traffic is traffic that is destined to a host group. Host groups for IPv4 multicast are identified by class D addresses, which range from 224.0.0.0 to 239.255.255.255.

**View, Search, or Clear the MFDB Table**

The Multicast Forwarding Database (MFDB) holds the port membership information for all active multicast address entries. The key for an entry consists of a VLAN ID and MAC address pair. Entries can contain data for more than one protocol.

**To view, search, or clear the MFDB Table:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.
The System Information page displays.

5. Select **Switching > Multicast > MFDB > MFDB Table**.

6. In the **Search by MAC Address** field, enter a MAC address.
   
Enter six two-digit hexadecimal numbers separated by colons, for example 00:01:23:43:45:67.

7. Click the **Go** button.
   
   If the address exists, the entry is displayed. An exact match is required.

8. To refresh the page with the latest information about the switch, click the **Refresh** button.

9. To clear all multicast forwarding address entries, click the **Clear** button.

**Table 41. MFDB table information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>The multicast MAC address for which you requested data.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID to which the multicast MAC address is related.</td>
</tr>
<tr>
<td>Type</td>
<td>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>Component</td>
<td>The component that is responsible for this entry in the Multicast Forwarding Database. The options are IGMP snooping, GMRP, Static Filtering, and MLD snooping.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description of this multicast table entry. The options are Management Configured, Network Configured, and Network Assisted.</td>
</tr>
<tr>
<td>Forwarding Interfaces</td>
<td>The resultant forwarding list is derived from combining all the forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.</td>
</tr>
</tbody>
</table>

**View the MFDB Statistics**

**To view the MFDB statistics:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Switching > Multicast > MFDB > MFDB Statistics.
   The MFDP Statistics page displays.

6. To refresh the page with the latest information about the switch, click the Refresh button.

The following table describes the MFDB Statistics fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max MFDB Table Entries</td>
<td>The maximum number of entries that the Multicast Forwarding Database table can hold (512 entries).</td>
</tr>
<tr>
<td>Most MFDB Entries Since Last Reset</td>
<td>The largest number of entries that were present in the Multicast Forwarding Database table since last reset. This value is also known as the MFDB high-water mark.</td>
</tr>
<tr>
<td>Current Entries</td>
<td>The current number of entries in the Multicast Forwarding Database table.</td>
</tr>
</tbody>
</table>

Configure the Auto-Video Multicast Settings

You can configure the auto-video multicast settings.

To configure auto-video multicast settings:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Switching > Multicast > Auto-Video.
The Auto-Video Configuration page displays.

6. Select one of the following radio buttons:
   • Select the **Disable** radio button to globally disable Auto-Video administrative mode for the switch.
   • Select the **Enable** radio button to globally enable Auto-Video administrative mode for the switch.

7. Click the **Apply** button.
   
   Your settings are saved.

   The Auto-Video VLAN field displays the Auto-Video VLAN ID that is configured on the switch. By default, this VLAN ID is 4089.

### About IGMP Snooping

Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward multicast traffic intelligently. Multicast IPv4 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 can 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 forwards a copy to 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 detected or processed by all connected nodes. For multicast packets, this approach could lead to a less efficient use of the network bandwidth, particularly when the packets are intended for a small number of nodes only. Packets are flooded into network segments where no node is receptive to the packet. Although nodes rarely incur any processing overhead to filter packets addressed to unrequested group addresses, the nodes cannot transmit new packets onto the shared media while the multicast packets are being flooded. Such as waste of bandwidth is even worse when the LAN segment is not shared, for example in full-duplex links.

Allowing switches to snoop IGMP packets can solve this problem. While the IGMP packets are being forwarded throughout the network, the switch uses the information in the packets to determine which segments must receive packets that are directed to the group address.
Configure IGMP Snooping

You can configure the settings for IGMP snooping, which is used to build forwarding lists for multicast traffic.

**To configure IGMP snooping:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address on page 12](#).
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **Switching > Multicast > IGMP Snooping > Configuration**.

6. Select the IGMP Snooping Status **Enable** or **Disable** radio button.
   This specifies the administrative mode for IGMP snooping for the switch. The default is **Disable**.

7. Select the Validate IGMP IP header **Enable** or **Disable** radio button.
   When IGMP IP header validation is enabled, any IGMP IP header must include the Router Alert, ToS, and TTL information. Otherwise, the IGMP packet is discarded. The default value is **Enable**.

8. Click the **Apply** button.
   Your settings are saved.

9. To refresh the page with the latest information about the switch, click the **Refresh** button.
The following table displays information about the global IGMP snooping status and statistics on the page.

### Table 43. IGMP Snooping Configuration information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast Control Frame Count</td>
<td>The number of multicast control frames that are processed by the CPU.</td>
</tr>
<tr>
<td>Interfaces Enabled for IGMP Snooping</td>
<td>The interfaces that are enabled for IGMP snooping.</td>
</tr>
<tr>
<td>VLAN IDs Enabled For IGMP Snooping</td>
<td>The IDs of the VLANs that are enabled for IGMP snooping.</td>
</tr>
<tr>
<td>VLAN IDs Enabled For IGMP Snooping Querier</td>
<td>The IDs of the VLANs that are enabled for IGMP snooping querier.</td>
</tr>
</tbody>
</table>

Configure IGMP Snooping for Interfaces

To configure IGMP snooping for interfaces:

1. Connect your computer to the same network as the switch.  
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.  
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch's password in the Password field.  
   The default password is password.

   The System Information page displays.

5. Select Switching > Multicast > IGMP Snooping > Interface Configuration.
6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   • 1 (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   • LAG. Only LAGs are displayed.
   • All. Both physical interfaces and LAGs are displayed.

7. Select one or more interfaces by taking one of the following actions:
   • To configure a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   • To configure multiple interfaces with the same settings, select the check box associated with each interface.
   • To configure all interfaces with the same settings, select the check box in the heading row.

8. From the Admin Mode menu, select Disable or Enable.
   This specifies the interface mode for the selected interface for IGMP snooping for the switch. The default is Disable.

9. In the Host Timeout field, specify the time that the switch must wait for a report for a particular group on a particular interface before it deletes that interface from the group.
   Enter a value between 1 and 3600 seconds. The default is 260 seconds.

10. In the Max Response Time field, specify the time that the switch must 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 group membership interval in seconds. The default is 10 seconds. The configured value must be less than the group membership interval.

11. In the MRouter Timeout field, specify the time that the switch must 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 time-out, that is, no expiration.

12. From the Fast Leave Mode menu, select whether fast leave mode is enabled.
    The option are Enable and Disable. The default is Disable.

13. Click the Apply button.
    Your settings are saved.
View, Search, or Clear the IGMP Snooping Table

You can view all of the entries in the Multicast Forwarding Database that were created for IGMP snooping.

To view, search, or clear the IGMP snooping table:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.
   
   The System Information page displays.

5. Select Switching > Multicast > IGMP Snooping > IGMP Snooping Table.
   
   The IGMP Snooping Table page displays.

6. In the Search By MAC Address field, specify the MAC address whose MFDB table entry you want to view.
   
   Enter six two-digit hexadecimal numbers separated by colons, for example 00:01:23:43:45:67.

7. Click the Go button.
   
   If the address exists, the entry is displayed. An exact match is required.

8. To refresh the page with the latest information about the switch, click the Refresh button.

9. To clear all multicast forwarding address entries that were created for IGMP snooping, click the Clear button.

The following table describes the information in the IGMP snooping table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>The multicast MAC address for which the switch holds forwarding and/or filtering information. The format is six 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>The VLAN ID for which the switch holds forwarding and filtering information.</td>
</tr>
</tbody>
</table>
To configure IGMP snooping settings for VLANs:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.
4. Enter the switch’s password in the Password field.
   
   The default password is password.

   The System Information page displays.
5. Select Switching > Multicast > IGMP Snooping > IGMP Snooping VLAN Configuration.

6. Select the check boxes for one or more VLANs.
   
   If you select the check box for a single VLAN, the VLAN ID displays in the VLAN ID field.
7. Configure the IGMP snooping values for the selected VLAN or VLANs:
   • **Admin Mode.** Enable or disable IGMP snooping for the specified VLAN ID. The default is Disable.
   • **Fast Leave Mode.** Enable or disable the IGMP snooping fast leave mode for the specified VLAN ID. The default is Disable.
   • **Host Timeout.** Set the value for group membership interval of IGMP snooping for the specified VLAN ID. The range is from the value for the Maximum Response Time plus 1 to 3600 seconds. The default is 260 seconds.
   • **Maximum Response Time.** Set the value for the maximum response time of IGMP snooping for the specified VLAN ID. The range is from 1 to the Host Timeout value minus 1. This value must be greater than group membership interval value. The default is 10 seconds.
   • **MRouter Timeout.** Set the value for multicast router expiry time of IGMP snooping for the specified VLAN ID. The range is from 0 to 3600 seconds. The default is 0 seconds.
   • **Report Suppression Mode.** Enable or disable IGMP snooping report suppression mode for the specified VLAN ID. IGMP snooping report suppression allows the suppression of the IGMP reports sent by the multicast hosts by building a Layer 3 membership table. The results is that only the most essential reports are sent to the IGMP routers so that the routers can continue to receive the multicast traffic. The default is Disable.
   • **Querier Mode.** Enable or disable the IGMP querier mode. The default is Disable.
   • **Query Interval.** Set the IGMP query interval for the specified VLAN ID. The range is from 1 to 1800 seconds. The default is 60 seconds.

8. Click the **Apply** button.
   Your settings are saved.

Modify IGMP Snooping Settings for a VLAN

**To modify IGMP snooping settings for a VLAN:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address on page 12.**
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
The System Information page displays.

5. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping VLAN Configuration**.
   
   The IGMP Snooping VLAN Configuration page displays.

6. Select the check box next to the VLAN ID.
7. Update the values.
8. Click the **Apply** button.

   Your settings are saved.

**Disable IGMP Snooping on a VLAN**

To disable IGMP snooping on a VLAN:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping VLAN Configuration**.
   
   The IGMP Snooping VLAN Configuration page displays.

6. Select the check box next to the VLAN ID.
7. From the **Admin Mode** menu, select **Disable**.
8. Click the **Apply** button.

   Your settings are saved.

**Configure a Multicast Router Interface**

You can configure an interface as the designated interface to which a multicast router is connected. All IGMP packets snooped by the switch are forwarded to the multicast router reachable from the interface. Configuring a multicast router interface is usually not required because the switch automatically detects the multicast router and forwards IGMP packets accordingly. This configuration is required only if you want to make sure that the multicast router always receives IGMP packets from the switch in a complex network.
To configure a multicast router interface:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.
   
   The System Information page displays.

5. Select Switching > Multicast > IGMP Snooping > Multicast Router Configuration.

   ![Multicast Router Configuration](image)

6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   
   • 1 (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   
   • LAG. Only LAGs are displayed.
   
   • All. Both physical interfaces and LAGs are displayed.

7. Select one or more interfaces by taking one of the following actions:
   
   • To configure a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   
   • To configure multiple interfaces with the same settings, select the check box associated with each interface.
   
   • To configure all interfaces with the same settings, select the check box in the heading row.

8. From the Multicast Router menu, select Enable or Disable.

9. Click the Apply button.
   
   Your settings are saved.
Configure a Multicast Router VLAN

You can configure an interface to forward only snooped IGMP packets from a specific VLAN to the multicast router connected to the interface. This configuration is usually not required because the switch automatically detects a multicast router and forwards the IGMP packets accordingly. This configuration is required only if you want to make sure that the multicast router always receives IGMP packets from the switch in a complex network.

To configure a multicast router VLAN:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
5. Select Switching > Multicast > IGMP Snooping > Multicast Router VLAN Configuration.

   ![Multicast Router VLAN Configuration](image)

6. From the Interface menu, select the interface.
7. In the VLAN ID field, enter the VLAN ID.
8. From the Multicast Router menu, select Enable or Disable.
9. Click the Apply button.
   Your settings are saved.
IGMP Snooping Querier Overview

IGMP snooping requires that one central switch or router periodically queries 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 stops forwarding multicasts to the port where the end device is located.

You can configure and display information about IGMP snooping queriers on the network and, separately, on VLANs.

Configure an IGMP Snooping Querier

You can configure the settings for an IGMP snooping querier.

To configure the settings for an IGMP snooping querier:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
5. Select Switching > Multicast > IGMP Snooping Querier > Querier Configuration.

6. Configure the following settings:
   - Querier Admin Mode. Enable or disable IGMP snooping for the switch. The default is Disable.
Configure an IGMP Snooping Querier for VLANs

You can configure IGMP queriers for use with VLANs on the network.

To configure IGMP snooping for a VLAN ID:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Switching > Multicast > IGMP Snooping Querier > Querier VLAN Configuration.

6. From the VLAN ID menu, select New Entry.
Configure the following settings:

- **VLAN ID.** The VLAN ID for which the IGMP snooping querier must be enabled. You can select an existing VLAN only.

- **Querier Election Participate Mode.** Enable or disable the querier mode:
  - **Disable.** Upon seeing another querier of the same version in the VLAN, the snooping querier moves to the non-querier state.
  - **Enable.** The snooping querier participates in querier election, in which the lowest 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 that are sent to the VLAN.

8. Click the **Apply** button.

Your settings are saved.

### Display IGMP Snooping Querier for VLAN Status

**To display querier VLAN status:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address on page 12](#).

   The login window opens.

4. Enter the switch's password in the **Password** field.
   
   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Status**.

6. To refresh the page with the latest information about the switch, click the **Refresh** button.
The following table describes the nonconfigurable information displayed on the page.

### Table 45. Querier VLAN Status information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID on which IGMP snooping querier is administratively enabled and the VLAN exists in the VLAN database.</td>
</tr>
<tr>
<td>Operational State</td>
<td>The operational state of the IGMP snooping querier on a VLAN. It can be in any of the following states:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Querier</strong>. The snooping switch is the querier in the VLAN. The snooping switch sends out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch finds a better querier 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 or when the querier address is not configured or the network management address is also not configured.</td>
</tr>
<tr>
<td>Operational Version</td>
<td>The operational IGMP protocol version of the querier.</td>
</tr>
<tr>
<td>Last Querier Address</td>
<td>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>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>The maximum response time to be used in the queries that are sent by the snooping querier.</td>
</tr>
</tbody>
</table>

### View, Search, and Manage the MAC Address Table

You can view or configure the MAC Address Table. This table contains information about unicast entries for which the switch holds forwarding or filtering information. This information lets the transparent bridging function determine how an incoming frame must be propagated.

If you clear the MAC address entries in the MAC Address Table, only the dynamic entries are removed.
View, Search, or Clear the MAC Address Table

To view, search, or clear the MAC Address Table:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.
   
   The System Information page displays.

5. Select Switching > Address Table > Basic > Address Table.

6. Use the Search menu and field to search for a MAC address, VLAN ID, or interface number:
   
   • Search by MAC Address. From the Search menu, select MAC Address, and enter the 6-byte hexadecimal MAC address in two-digit groups separated by colons, for example, 01:23:45:67:89:AB. Then click the Go button.
     
     If the address exists, that entry is displayed as the first entry followed by the remaining (higher) MAC addresses. An exact match is required.

   • Search VLAN ID. From the Search menu, select VLAN ID, and enter the VLAN ID, for example, 100. Then click the Go button.
• **Search Interface.** From the Search menu, select Interface, and enter the interface ID using the respective interface naming convention (for example, g1 or l1). Then click the Go button.

7. To refresh the page with the latest information about the switch, click the Refresh button.

8. To clear all dynamic MAC address entries in the table, click the Clear button.

The following table describes the nonconfigurable information displayed on the page.

**Table 46. MAC Address Table information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total MAC Address</td>
<td>The number of MAC addresses learned or configured.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID associated with the MAC address.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The unicast MAC address for which the switch holds forwarding and/or filtering information. The format is a 6-byte MAC address that is separated by colons, for example 01:23:45:67:89:AB.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface upon which this address was learned.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of this entry. The meanings of the values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Static. The value of the corresponding instance was added by the system or a user and cannot be relearned.</td>
</tr>
<tr>
<td></td>
<td>• Learned. The value of the corresponding instance was learned, and is being used.</td>
</tr>
<tr>
<td></td>
<td>• Management. The value of the corresponding instance is also the value of an existing instance of dot1dStaticAddress.</td>
</tr>
</tbody>
</table>

Set the Dynamic Address Aging Interval

You can set the address aging interval for the forwarding database.

**To set the address aging interval:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.
   
   The System Information page displays.
5. Select **Switching > Address Table > Advanced > Dynamic Addresses.**

![Dynamic Address Table](image)

6. In the **Address Aging Timeout (seconds)** field, specify the time-out period in seconds for aging out dynamically learned forwarding information. 802.1D-1990 recommends a default of 300 seconds. The value can be any number between 10 and 1000000 seconds. The default is 300.

7. Click the **Apply** button.

Your settings are saved.

---

**Add a Static MAC Address to the MAC Address Table**

To **add a static MAC address to the MAC Address Table:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch's password in the **Password** field.
   
   The default password is **password**.
   
   The System Information page displays.

5. Select **Switching > Address Table > Advanced > Static MAC Address.**

![Port List](image)

![Static MAC Address Table](image)

6. From the **Interface** menu, select the interface.
7. In the **Static MAC Address** field, enter the static MAC address that you want to add.

8. From the **VLAN ID** menu, select the VLAN ID that must be associated with the MAC address.

9. Click the **Add** button.

The static MAC address is added to the switch.

---

**Configure Layer 2 Loop Protection**

Loops inside a network are costly because they consume resources and reduce the performance of the network. Detecting loops manually can be cumbersome.

The switch can automatically identify loops in the network. You can enable loop protection per port or globally.

If loop protection is enabled, the switch sends predefined PDU packets to a Layer 2 broadcast destination address (FF:FF:FF:FF:FF:FF) on all ports for which the feature is enabled. You can selectively disable PDU packet transmission for loop protection on specific ports even while port loop protection is enabled. If the switch receives a packet with the previously mentioned broadcast destination address, the source MAC address in the packet is compared with the MAC address of the switch. If the MAC address does not match, the packet is forwarded to all ports that are members of the same VLAN, just like any other broadcast packet. The packet is not forwarded to the port from which it was received.

If the source MAC address matches the MAC address of the switch, the switch can perform one of the following actions, depending on how you configure the action:

- The port is shut down.
- A log message is generated. (If a syslog server is configured, the log message can be sent to the syslog server.)
- The port is shut down and a log message is generated.

Loop protection is not intended for ports that serve as uplinks between spanning tree–aware switches. It is intended for unmanaged switches that drop spanning tree BPDUs. Loop protection detects physical and logical loops between Ethernet ports on a device. You must enable loop protection globally before you can enable and configure it at the interface level. Loop protection is supported on physical interfaces and static LAG interfaces, but not on dynamic LAG interfaces.

---

**Configure Global Layer 2 Loop Protection**

*To configure L2 loop protection globally:*

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch's password in the **Password** field.
   The default password is **password**.
   The System Information page displays.
5. Select **Switching > L2 Loop Protection > L2 Loop Protection Configuration**.
   ![L2 Loop Protection Configuration](image)
6. To enable or disable loop protection feature, select the Admin Mode **Enable** or **Disable** radio button.
   By default, the **Disable** radio button is selected.
7. From the **Transmit Interval** menu, select the time in seconds between transmission of loop packets.
   The default transmit interval is 5 seconds.
8. From the **Max PDU Receive** menu, select the maximum number of packets to be received before an action is taken.
   The default is 1.
9. In the **Disable Timer** field, enter the time in seconds after which a port is disabled when a loop is detected.
   The range is from 0 to 604800 seconds. The default is 0 seconds.
10. Click the **Apply** button.
    Your settings are saved.

View and Configure Layer 2 Loop Protection on a Port

**To view and configure L2 loop protection on a port:**
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
5. Select Switching > L2 Loop Protection > L2 Loop Protection Configuration.
6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   • 1 (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   • LAG. Only LAGs are displayed.
   • All. Both physical interfaces and LAGs are displayed.
7. Select one or more interfaces by taking one of the following actions:
   • To configure a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   • To configure multiple interfaces with the same settings, select the check box associated with each interface.
   • To configure all interfaces with the same settings, select the check box in the heading row.
8. From the Keep Alive menu, select Enable or Disable to specify whether keep-alives are enabled on an interface.
   The default is Disable.
9. From the RX Action menu, select Log, Disable, or Both to specify the action that occurs when the switch detects a loop on an interface:
   • Log. The switch logs a message.
   • Disable. The switch disables the interface. This is the default action.
   • Both. The switch both logs a message and disables the interface.
10. Click the **Apply** button.
   Your settings are saved.

11. Click the **Clear** button to clear the statistics in the table.

12. Click the **Refresh** button to update the page to show the latest information.

The following table describes the nonconfigurable information displayed on the page.

**Table 47. L2 Loop Protection Interface Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loop Detected</td>
<td>Shows whether a loop is detected on the interface. If the interface is disabled and then reenabled, the status changes to No again.</td>
</tr>
<tr>
<td>Loop Count</td>
<td>The number of packets that were received after the loop was detected.</td>
</tr>
<tr>
<td>Time Since Last Loop</td>
<td>The time that elapsed since the loop was detected.</td>
</tr>
<tr>
<td>Port Status</td>
<td>The status of the interface (Enabled, Disabled, or D-Disabled, which stands for diagnostically disabled).</td>
</tr>
</tbody>
</table>
Configure Quality of Service

This chapter contains the following sections:

- Quality of Service Concepts
- Manage Class of Service
- Manage Differentiated Services
Quality of Service Concepts

In a 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 are held in the queue until the scheduler authorizes the queue for transmission. As queues become full, packets can no longer be held for transmission and are dropped by the switch.

Quality of Service (QoS) is a means of providing consistent, predictable data delivery by distinguishing packets with 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 that is not QoS capable creates a deficiency in the network path, and the performance of the entire packet flow is compromised.

Manage 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.

Note: Models GS324T and GS324TP support four hardware queues per port. Model GS348T supports eight hardware queues per port.

CoS Configuration Concepts

You can set the Class of Service trust mode for 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 must be forwarded on the appropriate egress port. Of course, the trusted field must exist in the packet for the mapping table to be of any use. If this is not the case, default actions are performed. 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 ports, in accordance with the configured default priority of the ingress port. This process is also used for cases where a trusted port mapping cannot be honored, such as when a non-IP packet arrives at a port configured to trust the IP DSCP value.

**Configure Global CoS Settings**

**To configure CoS trust mode settings on all interfaces:**

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   - The login window opens.
4. Enter the switch’s password in the Password field.
   - The default password is password.
   - The System Information page displays.

![CoS Configuration](image)

6. Either configure the same CoS trust mode settings for all CoS-configurable interfaces or configure CoS settings per interface.
   - By default, the Global radio button is selected.
     - To configure the same CoS trust mode settings for all CoS configurable interfaces, do the following:
       a. Select the Global radio button.
       b. From the Global Trust Mode menu, select one of the following trust mode options for ingress traffic on the switch:
          - Untrusted. Do not trust any CoS packet marking at ingress.
- **802.1p.** IEEE 802.1p specifies eight priority tags (p0 to p7). The QoS setting lets you map each of the eight priority levels to an internal hardware priority queue. Models GS324T and GS324TP support four hardware queues (0 to 3) and model GS348T supports eight hardware queues (0 to 7). The default mode is 802.1p.
- **DSCP.** The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.

7. Click the **Apply** button.
   Your settings are saved.

**Configure CoS Interface Settings for an Interface**

You can configure the trust mode for one or more interfaces and apply an interface shaping rate to all interfaces or to a specific interface.

**To configure CoS settings for an interface:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.
   The login window opens.

4. Enter the switch's password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - 1 (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - LAG. Only LAGs are displayed.
   - All. Both physical interfaces and LAGs are displayed.

7. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.

8. From the Interface Trust Mode menu, select one of the following trust mode options for ingress traffic on the selected interfaces:
   - Untrusted. Do not trust any CoS packet marking at ingress.
   - 802.1p. IEEE 802.1p specifies eight priority tags (p0 to p7). The QoS setting lets you map each of the eight priority levels to an internal hardware priority queue. Models GS324T and GS324TP support four hardware queues (0 to 3) and model GS348T supports eight hardware queues (0 to 7). The default mode is 802.1p.
   - DSCP. The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.

9. In the Interface Shaping Rate field, specify the maximum outbound transmission rate bandwidth in kbps.
   This setting is used to shape the outbound transmission rate in increments of 16 kbps in the range from 16 to 1,000,000 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. The value 0 means that the maximum is unlimited.

   The expected shaping at egress interface is calculated as follows:
   \[
   \text{frameSize} \times \text{shaping}/(\text{frameSize} + \text{IFG}), \text{where IFG (Inter frame gap) is 20 bytes, frameSize is configured frame size, and shaping is configured traffic shaping.}\]
For example, if 64 bytes frame size and 64 kbps shaping are configured, the expected shaping is approximately 48 kbps.

10. In the **Interface Ingress Rate Limit** field, specify the maximum inbound transmission rate bandwidth in kbps.

   This setting is used to shape the inbound transmission rate in increments of 16 kbps in the range from 16 to 1,000,000 kbps. The interface discards traffic that arrives at a bandwidth in excess of the specified limit.

11. Click the **Apply** button.

   Your settings are saved.

### Configure CoS Queue Settings for an Interface

You can 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 contains 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 configure CoS queue settings for an interface:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address** on page 12.

   The login window opens.

4. Enter the switch’s password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > CoS > Advanced > Interface Queue Configuration**.
6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - 1 (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - LAG. Only LAGs are displayed.
   - All. Both physical interfaces and LAGs are displayed.

7. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.

8. From the Queue ID menu, select the queue to be configured.

   Models GS324T and GS324TP support four queues (0 to 3) and model GS348T supports eight queues (0 to 7).

9. In the Minimum Bandwidth field, specify the minimum guaranteed bandwidth allotted to the queue.

   Setting this value higher than its corresponding maximum bandwidth automatically increases the maximum to the same value. The default value is 0. The range is 0 to 100 in increments of 1. The value 0 means no guaranteed minimum. The sum of the individual minimum bandwidth values for all queues for the interface cannot exceed the defined maximum (100).

10. From the Scheduler Type menu, select one of the following options:
    - Strict. The interface services traffic with the highest priority on a queue first.
    - Weighted. The interface uses weighted round robin to associate a weight to each queue. This is the default setting.

    The Queue Management Type field displays the queue depth management technique that is used for queues on the interface. By default, this method is Taildrop, irrespective of your selection from the Scheduler Type menu.
11. Click the **Apply** button.
Your settings are saved.

### Map 802.1p Priorities to Queues

You can view or change which internal traffic classes are mapped to the 802.1p priority class values in Ethernet frames that the device receives. The priority-to-traffic class mappings can be applied globally or per interface. The mapping allows the switch to group various traffic types (for example, data or voice) based on their latency requirements and give preference to time-sensitive traffic.

**To map 802.1p priorities to queues:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **QoS > CoS > Advanced > 802.1p to Queue Mapping**.

6. Specify whether the configuration applies to all interfaces that support CoS or to a single interface by selecting one of the following radio buttons:
   - **Global**. The configuration applies to all interfaces that can support CoS.
   - **Interface**. The configuration applies only to the interface that you must select from the **Interface** menu.

7. In the 802.1p to Queue Mapping table, map each of the eight 802.1p priorities to a queue (internal traffic class).
Models GS324T and GS324TP support four hardware queues (0 to 3) and model GS348T supports eight hardware queues (0 to 7). The default mode is 802.1p.

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 models GS324T and GS324TP or 7 for model GS348T). For example, traffic with a priority of 0 is for most data traffic and is sent using best effort. Traffic with a higher priority might be time-sensitive traffic, such as voice or video.

The values in the menu under each priority 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.

8. Click the Apply button.
Your settings are saved.

Map DSCP Values to Queues

You can map an internal traffic class to a DSCP value.

To map DSCP values to queues:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch's password in the Password field.
   The default password is password.
   The System Information page displays.
6. For each DSCP value, select from the corresponding **Queue** menu which internal traffic class must be mapped to the DSCP 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.

   The allowed Per Hop Behavior (PHBs) values, besides other DSCP experimental values, are as follows:

   - **Class Selector (CS) PHB**. These values are based on IP precedence.
   - **Assured Forwarding (AF) PHB**. These values define four main levels to sort and manipulate some flows within the network.
   - **Expedited Forwarding (EF) PHB**. These values are used to prioritize traffic for real-time applications. In many situations, if the network exceeded traffic and you need some bandwidth guaranteed for an application, the EF traffic must receive this rate independently of the intensity of any other traffic attempting to transit the node.

   The Other DSCP Values (Local/Experimental Use) section allows you to set non-default values for advanced settings.

7. Click the **Apply** button.

   Your settings are saved.

## Manage 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 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. If congestion occurs, packets might be delayed, sent sporadically, or dropped. For typical
Internet applications, such as email and file transfers, a slight degradation in service is acceptable and in many cases unnoticeable. However, any degradation of service can negatively affect applications with strict timing requirements, such as voice and multimedia.

Defining DiffServ

To use DiffServ for QoS, you must first 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 are defined by a class. The processing is defined by a policy's attributes. Policy attributes can 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.

Note the following about the DiffServ process:

- Packets are filtered and processed based on defined criteria. The filtering criteria is defined by a class. The processing is defined by a policy's attributes. Policy attributes can be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs.
- The configuration process begins with defining one or more match criteria for a class. Then one or more classes are added to a policy. Policies are then added to interfaces.
- Packet processing begins by testing the match criteria for a packet. The **All** class type option specifies that each match criteria within a class must evaluate to true for a packet to match that class. The **Any** class type option specifies that at least one match criteria must evaluate to true for a packet to match that class. Classes are tested in the order in which they were added to the policy. A policy is applied to a packet when a class match within that policy is found.

Configure and Display Global DiffServ Settings

You can 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 configure the global DiffServ mode and display DiffServ general status group information:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

The login window opens.

4. Enter the switch’s password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > DiffServ > Advanced > DiffServ Configuration**.

![DiffServ Configuration](image)

6. Select the administrative mode for DiffServ:
   - **Enable**. Differentiated services are active. This is the default setting.
   - **Disable**. The DiffServ configuration is retained and can be changed but is not active.

7. Click the **Apply** button.

   Your settings are saved.

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

**Table 48. DiffServ Status information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Table</td>
<td>The number of configured DiffServ classes out of the total allowed on the switch.</td>
</tr>
<tr>
<td>Class Rule table</td>
<td>The number of configured class rules out of the total allowed on the switch.</td>
</tr>
<tr>
<td>Policy table</td>
<td>The number of configured policies out of the total allowed on the switch.</td>
</tr>
<tr>
<td>Policy Instance table</td>
<td>The number of configured policy class instances out of the total allowed on the switch.</td>
</tr>
<tr>
<td>Policy Attributes table</td>
<td>The number of configured policy attributes (attached to the policy class instances) out of the total allowed on the switch.</td>
</tr>
<tr>
<td>Service table</td>
<td>The number of configured services (attached to the policies on specified interfaces) out of the total allowed on the switch.</td>
</tr>
</tbody>
</table>
Configure a DiffServ Class

You can add a new DiffServ class name, or rename or delete an existing class. You can also define the criteria to associate with a DiffServ class. As packets are received, these DiffServ classes are used to prioritize packets. You can set up 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.

Add and Configure a DiffServ Class

**To add and configure a DiffServ class:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the Password field.

   The default password is password.

   The System Information page displays.

5. Select QoS > DiffServ > Advanced > Class Configuration.

   The Class Name page displays.

6. In the Class Name field, enter a class name.

   The Class Name field also lists all existing DiffServ class names, from which you can select one for modification or deletion. The class name can be 1 to 31 alphanumeric characters in length.

   The switch supports only the class type value All, which means that all the various match criteria defined for the class are satisfied for a packet match. All signifies the logical AND statement of all the match criteria. For any class that you add, the class type is All.

7. Click the Add button.

   The new class is added.

8. After creating the class, click the class name.

   The class name is a hyperlink to the page on which you can define the class configuration.
Define the criteria that must be associated the DiffServ class by selecting one of the following radio buttons:

- **Match Every.** Select this radio button to add a match condition that considers all packets to belong to the class. The only selection from the Match Every menu is Any.
- **Reference Class.** Select this radio button to reference another class for criteria. The match criteria defined in the reference class function as match criteria in addition to the match criteria that you define for the selected class. After you select the radio button, the classes that can be referenced are displayed. Select the class to reference. A class can reference only one other class of the same type.
- **Class of Service.** Select this radio button to require the Class of Service (CoS) value in an Ethernet frame header to match the specified CoS value. This option lists all the values for the Class of Service match criterion in the range 0 to 7 from which you can select one.
- **VLAN.** Select this radio button to require a packet’s VLAN ID to match a VLAN ID. The VLAN value is in the range from 1 to 4093.
- **Ethernet Type.** Select this radio button to require the EtherType value in the Ethernet frame header to match the specified EtherType value. After you select the radio button, select the EtherType keyword from the menu of common protocols that are mapped to their Ethertype value. You can also select User Value from the menu and enter a value in the hexadecimal range from 600 to ffff.
• **Source MAC.** Select this radio button to require a packet’s source MAC address to match the specified MAC address. After you select this radio button, use the following fields to configure the source MAC address match criteria:
  - **Address.** The source MAC address to match. The source MAC address is specified as six two-digit hexadecimal numbers separated by colons.
  - **Mask.** The MAC mask, which specifies the bits in the source MAC address to compare against the Ethernet frame. Use Fs and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.

• **Destination MAC.** Select this radio button to require a packet’s destination MAC address to match the specified MAC address. After you select the radio button, use the following fields to configure the destination MAC address match criteria:
  - **Address.** The destination MAC address to match. The destination MAC address is specified as six two-digit hexadecimal numbers separated by colons.
  - **Mask.** The MAC mask, which specifies the bits in the destination MAC address to compare against an Ethernet frame. Use Fs and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.

• **Protocol Type.** Select this radio button to require a packet’s Layer 4 protocol to match the specified protocol, which you must select from the menu. You can also select **Other** from the menu and enter a protocol number from 0 to 255.

• **Source IP.** Select this radio button to require a packet’s source IP address to match the specified IP address. After you select the radio button, use the following fields to configure the source IP address match criteria:
  - **Address.** The source IP address format to match in dotted-decimal.
  - **Mask.** The bit mask in IP dotted-decimal format indicating which parts of the source IP address to use for matching against packet content.

• **Source L4 Port.** Select this radio button to require a packet’s TCP/UDP source port to match the specified protocol, which you must select from the menu. You can also select **Other** from the menu and enter a port number from 0 to 65535.

• **Destination IP.** Select this radio button to require a packet’s destination IP address to match the specified IP address. After you select the radio button, use the following fields to configure the destination IP address match criteria:
  - **Address.** The destination IP address format to match in dotted-decimal.
  - **Mask.** The bit mask in IP dotted-decimal format indicating which parts of the destination IP address to use for matching against packet content.
• **Destination L4 Port.** Select this radio button to require a packet’s TCP/UDP destination port to match the specified protocol. You can also select Other from the menu and enter a port number from 0 to 65535.

• **IP DSCP.** Select this radio button to require the packet’s IP DiffServ Code Point (DSCP) value to match the specified IP DSCP keyword code, which you must select from the menu. You can also select Other from the menu and enter an IP DSCP value from 0 to 63. The DSCP value is defined as the high-order 6 bits of the Service Type octet in the IP header.

• **Precedence Value.** Select this radio button to require the packet’s IP precedence value to match the specified number from 0 to 7, which you must select from the menu. The IP Precedence field in a packet is defined as the high-order 3 bits of the Service Type octet in the IP header.

• **IP ToS.** Select this radio button to require the packet’s Type of Service (ToS) bits in the IP header to match the specified value. The IP ToS field in a packet is defined as all 8 bits of the service type octet in the IP header. After you select the radio button, use the following fields to configure the ToS match criteria:
  - **Bits Value.** Enter a two-digit hexadecimal number octet value in the range from 00 to ff to match the bits in a packet’s ToS field.
  - **Bit Mask.** Specify the bit positions that are used for comparison against the IP ToS field in a packet.

10. Click the **Apply** button.

Your settings are saved.

The following table describes the nonconfigurable information displayed in the Class Summary section at the bottom of the DiffServ Class Configuration page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Match Criteria</strong></td>
<td>The configured match criteria for the specified class.</td>
</tr>
<tr>
<td><strong>Values</strong></td>
<td>The values of the configured match criteria.</td>
</tr>
</tbody>
</table>

**Rename an Existing DiffServ Class**

**To rename an existing DiffServ class:**

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **QoS > DiffServ > Advanced > Class Configuration**.
   The Class Name page displays.

6. Select the check box next to the class name.
7. In the **Class Name** field, specify the new name.
8. Click the **Apply** button.
   Your settings are saved.

Change the Criteria for an Existing DiffServ Class

**To change the criteria for an existing DiffServ class:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address on page 12](#).
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **QoS > DiffServ > Advanced > Class Configuration**.
   The Class Name page displays.

6. Click the class name, which is a hyperlink.
   The page on which you can change the class configuration displays.

7. Change the class configuration as needed.
8. Click the **Apply** button.
   Your settings are saved.
Delete a DiffServ Class

**To delete a DiffServ class:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **QoS > DiffServ > Advanced > Class Configuration**.
   The Class Name page displays.

6. Select the check box next to the class name.

7. Click the **Delete** button.
   The class is removed.

Configure a DiffServ Policy

You can associate a collection of classes with one or more policies.

Create and Configure a DiffServ Policy

**To create and configure a DiffServ policy:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
The System Information page displays.

5. **Select QoS > DiffServ > Advanced > Policy Configuration.**

The Policy Configuration page displays.

6. Enter a policy name in the **Policy Name** field.

   You cannot specify the policy type. By default, the policy type is In, indicating that the policy applies to ingress packets.

7. From the **Member Class** menu, optionally select an existing class that you want to associate with the new policy.

8. Click the **Add** button.

   The new policy is added.

9. After creating the policy, click the policy name.

   The policy name is a hyperlink to the page on which you can define the policy attributes.

10. **Configure the policy attributes by selecting one of the following radio buttons:**

    - **Assign Queue.** Select this radio button to specify that traffic must be assigned to a queue, which you must select from the menu. Models GS324T and GS324TP support four hardware queues (0 to 3) and model GS348T supports eight hardware queues (0 to 7).
• **Drop.** Select this radio button to require each inbound packet to be dropped.

• **Mark VLAN CoS.** Select this radio button to specify the VLAN priority, which you must select from the menu. The VLAN priority is expressed as a value in the range from 0 to 7.

• **Mark IP Precedence.** Select this radio button to require packets to be marked with an IP precedence value before being forwarded. You must select an IP precedence value from 0 to 7 from the menu.

• **Mirror.** Select this radio button to require packets to be mirrored to an interface or LAG, one of which you must select from the menu.

• **Redirect.** Select this radio button to require packets to be redirected to an interface or LAG, one of which you must select from the menu.

• **Mark IP DSCP.** Select this radio button to require packet to be marked with an IP DSCP keyword code, which you must select from the menu. The DSCP value is defined as the high-order 6 bits of the Service Type octet in the IP header.

• **Simple Policy.** Select this radio button to define the traffic policing style for the class. By default, this simple policy is color blind, and color classes do not apply. A simple policy supports a single data rate and a single burst size and results in one of two outcomes: conform or violate.

Specify a policy action for packets that conform or violate to the policy:

a. **Committed Rate.** Enter the committed rate that is applied to conforming packets by specifying a value in the range from 1 to 4294967295 Kbps.

b. **Committed Burst Size.** Enter the committed burst size that is applied to conforming packets by specifying a value in the range from 1 to 128 Kbps.

c. In the Conform Action section, select one of the following radio buttons:
   - **Send.** Packets are forwarded unmodified. This is the default confirming action.
   - **Drop.** Packets are dropped.
   - **Mark CoS.** Packets are marked by DiffServ with the specified CoS value before being forwarded. This selection requires that the Mark CoS field is set. You must select a CoS value from 0 to 7 from the menu.
   - **Mark IP Precedence.** These packets are marked by DiffServ with the specified IP Precedence value before being forwarded. This selection requires that the Mark IP Precedence field is set. You must select an IP precedence value from 0 to 7 from the menu.
   - **Mark IP DSCP.** Packets are marked by DiffServ with the specified DSCP value before being forwarded. This selection requires that the DSCP field is set. You must either select a DSCP code from the menu or enter an IP DSCP value from 0 to 63 in the field next to the menu. A value that you enter in the field overrides any selection from the menu.
      The DSCP value is defined as the high-order six bits of the Service Type octet in the IP header.
d. In the Violate Action section, select one of the following radio buttons:
   - **Send**. Packets are forwarded unmodified. This is the default violating action.
   - **Drop**. Packets are dropped.
   - **Mark CoS**. Packets are marked by DiffServ with the specified CoS value before being forwarded. This selection requires that the Mark CoS field is set. You must select a CoS value from 0 to 7 from the menu.
   - **Mark IP Precedence**. These packets are marked by DiffServ with the specified IP Precedence value before being forwarded. This selection requires that the Mark IP Precedence field is set. You must select an IP precedence value from 0 to 7 from the menu.
   - **Mark IP DSCP**. Packets are marked by DiffServ with the specified DSCP value before being forwarded. This selection requires that the DSCP field is set. You must either select a DSCP code from the menu or enter an IP DSCP value from 0 to 63 in the field next to the menu. A value that you enter in the field overrides any selection from the menu.

   The DSCP value is defined as the high-order six bits of the Service Type octet in the IP header.

11. Click the **Apply** button.
    Your settings are saved.

**Rename an Existing DiffServ Policy**

**To rename an existing DiffServ policy:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **QoS > DiffServ > Advanced > Policy Configuration**.
   The Policy Configuration page displays.

6. Select the check box next to the policy name.

7. In the **Policy Name** field, specify the new name.

8. Click the **Apply** button.
    Your settings are saved.
Change the Policy Attributes for an Existing DiffServ Policy

To change the policy attributes for an existing DiffServ policy:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.

   The System Information page displays.

5. Select QoS > DiffServ > Advanced > Policy Configuration.

   The Policy Configuration page displays.

6. Click the policy name, which is a hyperlink.

   The page on which you can change the policy attributes displays.

7. Change the policy attributes as needed.

8. Click the Apply button.

   Your settings are saved.

Remove a Class From an Existing DiffServ Policy

To remove a class from an existing DiffServ policy:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the Password field.

   The default password is password.

   The System Information page displays.
5. Select QoS > DiffServ > Advanced > Policy Configuration.  
The Policy Configuration page displays.
6. Select the check box next to the policy name.
7. From the Member Class menu, select None.
8. Click the Apply button.  
The class is removed from the policy.

Delete a DiffServ Policy

To delete a DiffServ policy:
1. Connect your computer to the same network as the switch.  
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.  
The default password is password.
   The System Information page displays.
5. Select QoS > DiffServ > Advanced > Policy Configuration.  
The Policy Configuration page displays.
6. Select the check box next to the policy name.
7. Click the Delete button.  
The policy is removed.

Configure the DiffServ Service Interface

You can assign (attach) a policy to an interface.

Attach a DiffServ Policy to an Interface

To attach a DiffServ policy to an interface:
1. Connect your computer to the same network as the switch.  
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
5. Select QoS > DiffServ > Advanced > Service Configuration.
6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   • 1 (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   • LAG. Only LAGs are displayed.
   • All. Both physical interfaces and LAGs are displayed.
7. Select one or more interfaces by taking one of the following actions:
   • To configure a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   • To configure multiple interfaces with the same settings, select the check box associated with each interface.
   • To configure all interfaces with the same settings, select the check box in the heading row.
8. From the Policy Name menu, select a policy name.
9. Click the Apply button.
   Your settings are saved.
The following table describes the nonconfigurable information displayed on the page.

**Table 50. Service Interface Configuration information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direction</td>
<td>Shows the traffic direction of this service interface, which is always inbound (In).</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Shows the operational status of this service interface (either Up or Down).</td>
</tr>
</tbody>
</table>

Remove a DiffServ Policy From an Interface

**To remove a DiffServ policy from an interface:**

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see *Discover or Change the Switch IP Address* on page 12.
   - The login window opens.
4. Enter the switch’s password in the **Password** field.
   - The default password is **password**.
   - The System Information page displays.
5. Select **QoS > DiffServ > Advanced > Service Configuration**.
   - The Service Interface Configuration page displays.
6. Select the check boxes that are associated with the interfaces from which you want to remove the policy.
7. From the **Policy In Name** menu, select **None**.
8. Click the **Apply** button.
   - Your settings are saved.

View DiffServ Service Statistics

You can display service-level statistical information about all interfaces to which DiffServ policies are attached.

**To view the DiffServ service statistics:**

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch's password in the Password field.
   
   The default password is password.
   
   The System Information page displays.

5. Select QoS > DiffServ > Advanced > Service Statistics.
   
   The Service Statistics page displays.

6. Click the Refresh button to refresh the page with the latest information about the switch.

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

**Table 51. DiffServ Service Statistics information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>All valid port numbers on the switch with a DiffServ policy that is attached in the inbound direction.</td>
</tr>
<tr>
<td>Direction</td>
<td>The traffic direction of interface is inbound (In). This field shows only the direction for which a DiffServ policy is attached.</td>
</tr>
<tr>
<td>Policy Name</td>
<td>The name of the policy that is currently attached to the specified interface and direction.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The operational status of the policy that is attached to the specified interface and direction. The value is either Up or Down.</td>
</tr>
<tr>
<td>Discarded packets</td>
<td>The number of packets that were discarded for all class instances in this service policy for any reason because of the DiffServ treatment. This is the overall count per interface, per direction. The number of discarded packets is displayed in the inbound direction only.</td>
</tr>
<tr>
<td>Member Classes</td>
<td>All DiffServ classes that are defined as members of the selected policy name. Select a member class name to display its statistics. If no class is associated with the selected policy, then the list is empty.</td>
</tr>
</tbody>
</table>
5

Manage Device Security

This chapter contains the following sections:

- Configure the Management Security Settings
- Configure Management Access
- Configure Port Authentication
- Set Up Traffic Control
- Configure Access Control Lists
Configure the Management Security Settings

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.

Change the Password for the Local Browser Interface

You can change the login password for the default user with the user name admin.

To change the login password for the local browser interface:

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   - The login window opens.
4. Enter the switch’s password in the Password field.
   - The default password is password.
   - The System Information page displays.
   - The Change Password page displays.
6. In the Current Password field, enter the current password.
   - The default password is password. The password is displayed in dots.
7. In the New Password field, specify the new password.
   - The password is displayed in dots. A password can be up to 20 alphanumeric characters in length, and is case-sensitive.
8. In the Confirm Password field, enter the password again to confirm that you entered it correctly.
   - The password is displayed in dots.
9. Click the Apply button.
   - Your settings are saved.
Note: If you forget the password and are unable to log in to the switch local browser interface, press the Factory Defaults button on the front panel of the switch for more than five seconds. The device reboots, and all switch settings, including the password, are reset to the factory default values.

Manage the RADIUS Settings

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 the following:

- Web access
- Access control port (802.1X)

Configure the Global RADIUS Server Settings

You can add information about one or more RADIUS servers on the network.

If you configure multiple RADIUS servers, consider the maximum delay time when you specify the maximum number of retransmissions (that is, the value that you enter in the Max Number of Retransmits field) and the time-out period (that is, the value that you enter in the Timeout Duration field) for RADIUS:

For one RADIUS server, a retransmission does not occur until the configured time-out period expires without a response from the RADIUS server. In addition, the maximum number of retransmissions for one RADIUS server must pass before the switch attempts the next RADIUS server.

Therefore, the maximum delay in receiving a RADIUS response on the switch equals the maximum number of retransmissions multiplied by the time-out period multiplied by the number of configured RADIUS servers. If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the switch receives a RADIUS response.

To configure the global RADIUS server settings:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
The login window opens.

4. Enter the switch’s password in the **Password** field.

The default password is **password**.

The System Information page displays.

5. Select **Security > Management Security > RADIUS > Global Configuration**.

The Current Server IP Address field is blank if no servers are configured (see Configure a RADIUS Authentication Server on the Switch on page 213). The switch supports up to three RADIUS servers. If more than one RADIUS server is 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.

![RADIUS Configuration](image)

**CAUTION:**

The maximum delay in receiving a RADIUS response on the switch equals the maximum number of retransmissions multiplied by the time-out period multiplied by the number of configured RADIUS servers. If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the switch receives a RADIUS response.

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

   The range is from 1 to 15. The default value is 4.

7. In the **Timeout Duration** field, specify the time-out value, in seconds, for request retransmissions.

   The range is from 1 to 30. The default value is 5.

8. From the **Accounting Mode** menu, select to disable or enable RADIUS accounting on the server.

   The default is Disabled.

9. Click the **Apply** button.

   Your settings are saved.
The following table describes the nonconfigurable fields displayed on the page.

**Table 52. RADIUS Configuration information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Server IP Address</td>
<td>The IP address of the current server. This field is blank if no servers are configured.</td>
</tr>
<tr>
<td>Number of Configured Servers</td>
<td>The number of configured authentication RADIUS servers. The value can range from 0 to 32.</td>
</tr>
</tbody>
</table>

Configure a RADIUS Authentication Server on the Switch

You view and configure various settings for a RADIUS server configured on the switch.

Add a Primary RADIUS Authentication Server to the Switch

**To add a primary RADIUS authentication server to the switch and view or reset the RADIUS authentication server statistics:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.

   The System Information page displays.

5. **Select** **Security > Management Security > RADIUS > Server Configuration**.

6. In the **Server Address** field, specify the IP address of the RADIUS server.

7. In the **Authentication Port** field, specify the UDP port number that the server uses to verify the RADIUS server authentication.
   
   The range is from 1 to 65535. The default value is 1812.
8. From the **Secret Configured** menu, select **Yes**.
   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 was configured.

9. 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.

10. From the **Active** menu, select **Primary**.
11. From the **Message Authenticator** menu, select **Enable** or **Disable** to specify whether the message authenticator attribute for the selected server is enabled.
   The message authenticator adds protection to RADIUS messages by using an MD5 hash to encrypt each message. The shared secret is used as the key, and if the message fails to be verified by the RADIUS server, it is discarded.
12. Click the **Add** button.
   The server is added to the switch.

13. To reset the authentication server and RADIUS statistics to their default values, click the **Clear Counters** button.

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

**Table 53. RADIUS authentication server statistics information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
<td>The address of the RADIUS server or the name of the RADIUS server for which the statistics are displayed.</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>
<tr>
<td>Access Requests</td>
<td>The number of RADIUS access-request packets sent to this server. This number does not include retransmissions.</td>
</tr>
<tr>
<td>Access Retransmissions</td>
<td>The number of RADIUS access-request packets retransmitted to this server.</td>
</tr>
<tr>
<td>Access Accepts</td>
<td>The number of RADIUS access-accept packets, including both valid and invalid packets, that were received from this server.</td>
</tr>
<tr>
<td>Access Rejects</td>
<td>The number of RADIUS access-reject packets, including both valid and invalid packets, that were received from this server.</td>
</tr>
<tr>
<td>Access Challenges</td>
<td>The number of RADIUS access-challenge packets, including both valid and invalid packets, that were received from this server.</td>
</tr>
<tr>
<td>Malformed Access Responses</td>
<td>The number of malformed RADIUS access-response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included in malformed access-responses.</td>
</tr>
</tbody>
</table>
Modify the Settings for a RADIUS Authentication Server on the Switch

To modify the settings for a RADIUS authentication server on the switch:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

   The Server Configuration page displays.

6. Select the check box next to the server IP address.

7. Modify the configuration for the selected server.

8. Click the Apply button.
   Your settings are saved.

---

### Table 53. RADIUS authentication server statistics information (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad Authenticators</td>
<td>The number of RADIUS access-response packets containing invalid authenticators or signature attributes received from this server.</td>
</tr>
<tr>
<td>Pending Requests</td>
<td>The number of RADIUS access-request packets destined for this server that did not yet time out or receive a response.</td>
</tr>
<tr>
<td>Timeouts</td>
<td>The number of authentication time-outs to this server.</td>
</tr>
<tr>
<td>Unknown Types</td>
<td>The number of RADIUS packets of unknown type that were received from this server on the authentication port.</td>
</tr>
<tr>
<td>Packets Dropped</td>
<td>The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.</td>
</tr>
</tbody>
</table>
Remove a RADIUS Authentication Server From the Switch

To remove a RADIUS authentication server from the switch:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
   The Server Configuration page displays.
6. Select the check box next to the IP address of the server to remove.
7. Click the Delete button.
   The RADIUS server is removed.
8. Click the Apply button.
   Your settings are saved.

Configure a RADIUS Accounting Server
You can view and configure various settings for a RADIUS accounting server on the network.

Add a RADIUS Accounting Server to the Switch

To add a RADIUS accounting server to the switch and view or clear the RADIUS accounting server statistics:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the **Password** field.
   
The default password is **password**.
   
The System Information page displays.

5. Select **Security > Management Security > RADIUS > Accounting Server Configuration**.

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

7. In the **Port** field, specify the UDP port number that the server uses to verify the RADIUS accounting server authentication. The default UDP port number is 1813.

8. From the **Secret Configured** menu, select **Yes** to add a RADIUS secret in the next field or select **No** to ignore the RADIUS secret.

   To configure the RADIUS secret, you must select **Yes**. After you add the RADIUS accounting server, this field indicates whether the shared secret for this server was configured.

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

10. From the **Accounting Mode** menu, select **Enable** to enable the RADIUS accounting mode.

11. Click the **Add** button.

   The server is added to the switch.

12. To reset the accounting server and RADIUS statistics to their default values, click the **Clear Counters** button.

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

**Table 54. RADIUS accounting server statistics information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Server Address</td>
<td>The accounting server associated with the statistics.</td>
</tr>
<tr>
<td>Round Trip Time (secs)</td>
<td>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 not including retransmissions.</td>
</tr>
<tr>
<td>Accounting Retransmissions</td>
<td>The number of RADIUS accounting-request packets retransmitted to this RADIUS accounting server.</td>
</tr>
</tbody>
</table>
To modify the settings for a RADIUS accounting server on the switch:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

   The Accounting Server Configuration page displays.

6. Select the check box next to the server IP address.

7. Modify the configuration for the selected accounting server.

8. Click the Apply button.
   Your settings are saved.
Remove a RADIUS Accounting Server From the Switch

**To remove a RADIUS accounting server from the switch:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address on page 12](#).
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.
   
   The System Information page displays.

5. Select **Security > Management Security > RADIUS > Accounting Server Configuration**.
   
   The Accounting Server Configuration page displays.

6. Select the check box next to the server IP address.

7. Click the **Delete** button.
   
   Your settings are saved. The RADIUS accounting server is removed.

Configure 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 through 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.
Configure the Global TACACS+ Settings

You can configure the global TACACS+ settings for communication between the switch and a TACACS+ server.

To configure the global TACACS+ settings:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.


6. In the Key String field, specify the authentication and encryption key for TACACS+ communications between the switch and the TACACS+ server.
   The range is from 0 to 128. The key must match the key configured on the TACACS+ server.

7. In the Connection Timeout field, specify the maximum number of seconds allowed to establish a TCP connection between the switch and the TACACS+ server.
   The range is from 1 to 30 seconds. The default is 5 seconds.

8. Click the Apply button.
   Your settings are saved.
Configure a TACACS+ Server on the Switch
You can configure up to three TACACS+ servers with which the switch can communicate.

**To configure a TACACS+ server on the switch:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **Security > Management Security> TACACS+ > TACACS+ Server Configuration**.

6. In the **TACACS+ Server** field, enter the TACACS+ server IP address.

7. In the **Priority** field, specify the priority for the TACACS+ server.
   The priority determines the order in which the TACACS+ servers are contacted when attempting to authenticate a user. A value of 0 is the highest priority. The range is from 0 to 65535.

8. In the **Port** field, specify the authentication port value for TACAS+ server sessions.
   The value must be in the range from 0 to 65535. If you do not specify a value, the switch uses the standard TCP port 49 for sessions with the server.

9. In the **Key String** field, specify the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server.
   The range is from 0 to 128. The key must match the key used on the TACACS+ server.

10. In the **Connection Timeout** field, specify the time that passes before the connection between the device and the TACACS+ server times out.
    The range is from 1 to 30. If you do not specify a value, the switch uses a default value of 5 seconds.

11. Click the **Add** button.
    The server is added to the switch.
Modify the Settings for a TACACS+ Server on the Switch

To modify the settings for a TACACS+ server on the switch:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
   The TACACS+ Server Configuration page displays.
6. Select the check box next to the server IP address.
7. Modify the configuration for the selected TACACS+ server.
8. Click the Apply button.
   Your settings are saved.

Remove a TACACS+ Server From the Switch

To remove a TACACS+ server from the switch:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
The TACACS+ Server Configuration page displays.

6. Select the check box next to the server IP address.
7. Click the Delete button.
   The TACACS+ server is removed.

Configure Authentication Lists

You can configure a default login list. A login list specifies one or more authentication methods to validate switch or port access for the admin user.

---

**Note:** The admin user is assigned to a preconfigured list that is named defaultList and that you cannot delete.

---

Configure an HTTP Authentication List

You can configure the default HTTP login list.

**To change the HTTP authentication method for the default list:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.


6. Select the check box next to the httpList name.
7. From the menu in the 1 column, select the authentication method that must be used 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 is tried, even if you specified more than one method. User authentication occurs in the order the methods are selected. Possible methods are as follows:

- **Local**. The user’s locally stored ID and password are used for authentication. Since the Local method does not time out, if you select this option as the first method, no other method is tried, even if you specified more than one method. This is the default method. This is the default selection for Method 1.

- **RADIUS**. The user’s ID and password are 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 are 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, that is, no authentication is required.

8. From the menu in the 2 column, select the authentication method, if any, that must be used second in the selected authentication login list.

   This is the method that is used if the first method times out. If you select a method that does not time out as the second method, the third method is not tried.

9. From the menu in the 3 column, select the authentication method, if any, that must be used third in the selected authentication login list.

10. From the menu in the 4 column, select the method, if any, that must be used fourth in the selected authentication login list.

   This is the method that is used if all previous methods time out.

11. Click the **Apply** button.

    Your settings are saved.

Configure an HTTPS Authentication List

You can configure the default login list for secure HTTP (HTTPS).

**To configure an HTTPS authentication list:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.

   The login window opens.

4. Enter the switch’s password in the **Password** field.
The default password is **password**.

The System Information page displays.

5. Select **Security > Management Security > Authentication List > HTTPS Authentication List**.

6. Select the check box next to the httpsList name.

7. From the menu in the 1 column, select the authentication method that must be used 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 is tried, even if you specified more than one method. This setting does not display 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 are used for authentication. Since the Local method does not time out, if you select this option as the first method, no other method is tried, even if you specified more than one method. This is the default selection for Method 1.

   - **RADIUS**: The user’s ID and password are 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 are 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, that is, no authentication is required.

8. From the menu in the 2 column, select the authentication method, if any, that must be used second in the selected authentication login list.

   This is the method that is used if the first method times out. If you select a method that does not time out as the second method, the third method is not tried.

9. From the menu in the 3 column, select the authentication method, if any, that must be used third in the selected authentication login list.

10. From the menu in the 4 column, select the method, if any, that must be used fourth in the selected authentication login list.

   This is the method that is used if all previous methods time out.

11. Click the **Apply** button.

    Your settings are saved.
Configure the Dot1x Authentication List

The Dot1x authentication list defines the IEEE 802.1X authentication method used for the default list. The default list is dot1xList.

To configure the dot1x authentication list:

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   - The login window opens.

4. Enter the switch’s password in the Password field.
   - The default password is password.
   - The System Information page displays.

   - The Dot1x Authentication List page displays.

6. Select the check box next to dot1xList.

7. From the menu in the 1 column, select the method that must be used first in the selected authentication login list.
   - The options are as follows:
     - **Local.** The user’s locally stored ID and password are used for authentication
     - **Radius.** The user’s ID and password are authenticated using the RADIUS server instead of locally.
     - **None.** The user is not authenticated.

8. Click the Apply button.
   - Your settings are saved.
Manage the Smart Control Center Utility

You can enable or disable the SCC administrative mode.

**To enable or disable the SCC administrative mode:**

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.
   - The login window opens.
4. Enter the switch’s password in the **Password** field.
   - The default password is **password**.
   - The System Information page displays.
5. Select **Security > Management Security > SCC Control**.
   - The NETGEAR Smart Control Center (SCC) Utility page displays.
6. Select the one of the following SCC Admin Mode radio buttons:
   - **Enable**. SCC can discover the switch and perform actions on the switch. This is the default setting.
   - **Disable**. SCC can discover the switch but cannot perform any actions on the switch.

   **Note**: Because the switch administrator password is contained in each NETGEAR Switch Discovery Protocol (NSDP) packet, disabling SCC increases the switch security.
7. Click the **Apply** button.
   - Your settings are saved.

Configure Management Access

You can configure HTTP and secure HTTP access to the switch local browser interface. You can also configure access control profiles and access rules.
Configure HTTP Access Settings

You can configure the HTTP access settings on the switch.

To configure the HTTP access settings:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Security > Access > HTTP > HTTP Configuration.

6. In the HTTP Session Soft Timeout field, specify the number of minutes an HTTP session can be idle before a time-out occurs.
   The value must be in the range from 0 to 60 minutes. The default value is 5 minutes.
   After the session is inactive for the configured time, you are automatically logged out and must reenter the password to access the local browser interface. A value of zero means that the session does not time out.

7. In the HTTP Session Hard Timeout field, specify the hard time-out for HTTP sessions.
   This time-out is unaffected by the activity level of the session. The value must be in the range from 0 to 168 hours. A value of zero means that the session does not time out. The default value is 24 hours.

8. In the Maximum Number of HTTP Sessions field, specify the maximum number of HTTP sessions that can exist at the same time.
   The range is from 1 to 4 sessions. The default is 4 sessions.

9. Click the Apply button.
   Your settings are saved.
Configure HTTPS Access Settings

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. The hash algorithms that SSL uses are MD5 and SHA-1.

To configure HTTPS access settings:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.
   
   The System Information page displays.

5. Select Security > Access > HTTPS > HTTPS Configuration.

6. Select the Admin Mode Enable or Disable radio button.
   
   This selection enables or disables secure HTTP (HTTPS). The default value is Disable. You can download SSL certificates only when HTTPS is disabled. You can enable HTTPS only if a certificate is present on the device.

7. Select the SSL Version 3 Enable or Disable radio button.
   
   This selection enables or disables Secure Sockets Layer version 3.0. The default value is Enable.

8. Select the TLS Version 1 Enable or Disable radio button.
   
   This selection enables or disables Transport Layer Security (TLS) version 1.0 and TLS version 1.2. The default value is Enable.
9. In the **HTTPS Port** field, type the HTTPS port number.
   The range is from 1025 to 65535. The default is port 443.

10. In the **HTTPS Session Soft Timeout (Minutes)** field, enter the inactivity time-out for HTTPS sessions.
    The range is from 1 to 60 minutes. The default value is 5 minutes.

11. In the **HTTPS Session Hard Timeout (Hours)** field, set the hard time-out for HTTPS sessions.
    This time-out is unaffected by the activity level of the session. The range is from 1 to 168 hours. The default is 24 hours.

12. In the **Maximum Number of HTTPS Sessions** field, enter the maximum allowable number of HTTPS sessions.
    The range is from 1 to 4 sessions. The default is 4 sessions.

13. Click the **Apply** button.
    Your settings are saved.

Manage Certificates for HTTPS Access

You can manage certificates for HTTPS access.

Generate an SSL Certificate

---

**Note:** If you use HTTPS access, before you can generate a certificate, you must disable HTTPS (see Configure HTTPS Access Settings on page 229) and log back in to the local browser interface over an HTTP session. After you generate the certificate, you can reenable HTTPS and log back in to the local browser interface over an HTTPS session.

---

**To generate an SSL certificate:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **Security > Access > HTTPS > Certificate Management**.

   ![Certificate Management](image)

   The Certificate Present field displays whether a certificate is present on the switch.

6. In the Certificate Management section, select the **Generate Certificates** radio button.

7. Click the **Apply** button.
   The switch generates an SSL certificate.
   The Certificate Generation Status field shows progress information.

### Delete an SSL Certificate

**Note:** If you use HTTPS access, before you can delete a certificate, you must disable HTTPS (see Configure HTTPS Access Settings on page 229) and log back in to the local browser interface over an HTTP session. After you generate the certificate, you can reenable HTTPS and log back in to the local browser interface over an HTTPS session.

**To delete an SSL certificate:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **Security > Access > HTTPS > Certificate Management**.

   The Certificate Present field displays **Yes**.

7. In the Certificate Management section, select **Delete Certificates** radio button.

8. Click the **Apply** button.
   The certificate is removed.

Transfer an Existing Certificate to the Switch

You can transfer a certificate file to the switch.

For the switch to accept HTTPS connections from a device, the switch requires a public key certificate. You can generate a certificate externally (for example, offline) and transfer it to the switch.

Before you transfer a file from a TFTP server to the switch, the following conditions must be true:

- The file that you transfer from a TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch contains a path to the TFTP server.

---

**Note:** If you use HTTPS access, before you can transfer a certificate, you must disable HTTPS (see **Configure HTTPS Access Settings** on page 229) and log back in to the local browser interface over an HTTP session. After you generate the certificate, you can reenable HTTPS and log back in to the local browser interface over an HTTPS session.

---

**To configure the certificate transfer settings for HTTPS sessions:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address** on page 12.
The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. **Select Security > Access > HTTPS > Certificate Download.**

   ![Certificate Download](image)

6. From the **File Type** menu, select the type of SSL certificate to download, which can be one of the following:
   - **SSL Trusted Root Certificate PEM File.** SSL Trusted Root Certificate file (PEM Encoded)
   - **SSL Server Certificate PEM File.** SSL Server Certificate File (PEM Encoded)
   - **SSL DH Weak Encryption Parameter PEM File.** SSL Diffie-Hellman Weak Encryption Parameter file (PEM Encoded)
   - **SSL DH Strong Encryption Parameter PEM File.** SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded)

7. From the **Server Address Type** menu, select **IPv4** or **DNS** to indicate the format for the TFTP Server IP field.
   The default is IPv4.

8. In the **TFTP Server IP** field, specify the address or host name of the TFTP server.
   The address can be an IP address in standard x.x.x.x format or a host name. The host name must start with a letter of the alphabet.

9. In the **Remote File Path** field, enter the path of the file to download.
   You can enter up to 96 characters. The default is blank.

10. In the **Remote File Name** field, enter the name of the file on the TFTP server to download.
    You can enter up to 32 characters. The default is blank.

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

12. **Click the Apply button.**
    The file transfer starts. A status message displays during the transfer and upon successful completion of the transfer.
Manage Access Control to the Switch

Access control allows you to configure an access control profile and set rules for access to the local browser interface, access by SNMP stations, SNTP devices, and client access to a TFTP server. We refer to an access control profile as an access profile. You can add a single access profile, which you can configure, activate, or deactivate.

**CAUTION:**
If you configure a security access profile incorrectly and you activate the access profile, you might no longer be able to access the switch’s local browser interface. If that situation occurs, you must reset the switch to factory default settings (see Reset the Switch to Its Factory Default Settings on page 324).

Add an Access Profile
You can set up a single security access profile with which you can associate an access rule configuration.

**To add an access profile:**
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
6. In the **Access Profile Name** field, enter the name of the access profile to be added. The maximum length is 32 characters.

7. Click the **Apply** button.

Your settings are saved. By default, the access profile is deactivated. After you add rules, you can activate the access profile.

---

Add a Rule to the Access Profile

After you add the access profile, you can add one or more security access rules to the access profile.

---

**CAUTION:**

You must add a permit rule for your device and access method, otherwise you are locked out from the switch after you activate the access profile. If that situation occurs, you must reset the switch to factory default settings (see Reset the Switch to Its Factory Default Settings on page 324).  

---

To add a rule to the access profile:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Security > Access > Access Control > Access Rule Configuration.**

![Access Rule Configuration](image)

6. From the **Rule Type** menu, select **Permit** or **Deny** to permit or deny access when the selected rules are matched.

   A Permit rule allows access from a device that matches the rule criteria. A Deny rule blocks a device that matches the rule criteria.

7. From the **Service Type** menu, select the access method to which the rule is applied.

   The policy is restricted by the selected access method. Possible access methods are TFTP, HTTP, Secure HTTP (SSL), SNMP, and SNTP.

8. In the **Source IP Address** field, enter the source IP address from which the management traffic originates.

9. In the **Mask** field, specify the subnet mask from which the management traffic originates.

10. In the **Priority** field, assign a priority to the rule.

    The rules are validated against the incoming management request in ascending order of their priorities. If a rule matches, the action is performed and subsequent rules below that rule are ignored. For example, if a source IP address 10.10.10.10 is configured with priority 1 to permit, and the same source IP address 10.10.10.10 is also configured with priority 2 to deny, then access is permitted if the profile is active, and the second rule is ignored.

11. Click the **Add** button.

    The access rule is added.

---

**Activate the Access Profile**

After you add rules to the access profile, you can activate the access profile.

---

**CAUTION:**

If you configure a security access profile incorrectly and you activate the access profile, you might no longer be able to access the switch’s local browser interface. If that situation occurs, you must reset the switch to factory default settings (see **Reset the Switch to Its Factory Default Settings** on page 324).

**To activate the access profile:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
   The Access Profile Configuration page displays. The Deactivate Profile check box is selected.
6. Select the Activate Profile check box.
7. Click the Apply button.
   Your settings are saved and the access profile is now active.

Display the Access Profile Summary and the Number of Filtered Packets
After you added rules to the active profile, you can view the entries in the summary. If the access profile is active, you can also view the number of filtered packets.

To display the access profile summary and the number of filtered packets:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
The Packets Filtered field displays the number of packets filtered (none in the previous figure).

6. To refresh the page with the latest information about the switch, click the **Refresh** button.

The following table describes the nonconfigurable data that is displayed.

**Table 55. Access profile configuration profile summary**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Type</td>
<td>The action performed when the rules match.</td>
</tr>
<tr>
<td>Service Type</td>
<td>The service type selected. The policy is restricted by the selected service type.</td>
</tr>
<tr>
<td>Source IP Address</td>
<td>The source IP address of the client originating the management traffic.</td>
</tr>
<tr>
<td>Mask</td>
<td>The subnet mask of the IP Address.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority of the rule.</td>
</tr>
</tbody>
</table>

Deactivate an Access Profile

You can deactivate an access profile.

**To deactivate an access profile:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see *Discover or Change the Switch IP Address* on page 12.
The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **Security > Access > Access Control > Access Profile Configuration**.
   The Access Profile Configuration page displays. The **Activate Profile** check box is selected.

6. Select the **Deactivate Profile** check box.
7. Click the **Apply** button.
   Your settings are saved and the access profile is now deactivated.

Remove an Access Profile

You can remove an access profile that you no longer need. Before you can remove the access profile, you must deactivate it (see **Deactivate an Access Profile** on page 238).

**To remove an access profile:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address** on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **Security > Access > Access Control > Access Profile Configuration**.
   The Access Profile Configuration page displays. The **Deactivate Profile** check box is selected.

6. Select the **Remove Profile** check box.
7. Click the **Apply** button.
   The access profile is removed.
Configure Port Authentication

With port-based authentication, 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 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.

An 802.1X network includes three components:

- **Authenticator.** The port that is authenticated before access to system services is permitted.
- **Supplicant.** The host that is connected to the authenticated port requesting access to the system services.
- **Authentication Server.** The external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the supplicant is authorized to access system services.

Configure Global 802.1X Settings

You can configure global port access control settings on the switch.

**To globally enable the 802.1X features:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.

   The System Information page displays.

5. Select **Security > Port Authentication > Basic > 802.1X Configuration**.
6. Configure the following port authentication settings:

- **Port Based Authentication State.** This selection specifies the 802.1X administrative mode on the switch. The default value is Disable.
  - **Enabled.** If 802.1X is enabled, authentication is performed by a RADIUS server. This means that the primary authentication method must be RADIUS. To set the method, select **Security > Management Security > Authentication List** and select RADIUS as method 1 for defaultList. For more information, see Configure Authentication Lists on page 223.
  - **Disabled.** When port-based authentication is globally disabled, 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.

- **VLAN Assignment Mode.** This selection specifies whether a port can be placed in a particular VLAN. The default value is Disable.
  
  When enabled, this feature allows a port to be placed into a particular VLAN based on the result of the authentication or type of 802.1X authentication a client uses when it accesses the device. The authentication server can provide information to the device about which VLAN to assign the supplicant.

- **Dynamic VLAN Creation Mode.** This selection specifies whether a VLAN can be dynamically created. The default value is Disable.
  
  If RADIUS-assigned VLANs are enabled, the RADIUS server includes the VLAN ID in the 802.1X tunnel attributes of its response message to the device. If dynamic VLAN creation is enabled on the device and the RADIUS-assigned VLAN does not exist, the assigned VLAN is dynamically created. This means that the client can connect from any port and is assigned to the appropriate VLAN. This feature gives flexibility for clients to move around the network without much additional configuration required.

- **EAPOL Flood Mode.** This selection specifies whether Extensible Authentication Protocol (EAP) over LAN (EAPoL) flood support is enabled on the switch. The default value is Disable.

7. Click the **Apply** button.

Your settings are saved.

The protocol version associated with the selected port. The only possible value is 1, corresponding to the first version of the 802.1X specification.
Manage Port Authentication on Individual Ports

You can enable and configure port access control on one or more physical ports.

Configure 802.1X Settings for a Port

To configure 802.1X settings for a port:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.
   
   The System Information page displays.


   The previous figure does not show all columns on the page.

6. Select one or more interfaces by taking one of the following actions:
   
   • To configure a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   
   • To configure multiple interfaces with the same settings, select the check box associated with each interface.
   
   • To configure all interfaces with the same settings, select the check box in the heading row.

7. Specify the following settings:
**Port Control.** Defines the port authorization state. The control mode is set only if the link status of the port is link up. Select one of the following options:

- **Auto.** The switch automatically detects the mode of the interface.
- **Authorized.** The switch places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication.
- **Unauthorized.** The switch 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.

**Host Mode.** Defines the host mode for an interface. The host mode determines the number and types of clients that can be authenticated and authorized on the interface. The host mode can distinguish between data and voice clients. Select one of the following options:

- **Single-Host.** A single data client only can be authenticated and authorized on the interface before this client is granted access to the interface. Only after the client logs off, can another client be authenticated and authorized on the interface, and granted access to the interface.
- **Multi-Host.** After one data client is authenticated and authorized on the interface, access is granted to all clients that are connected to the interface.

For example, you can this mode if a WiFi access point is connected to an access-controlled port of a NAS. After the access point is authenticated by the NAS, the interface is authorized for traffic of all WiFi clients that are connected to the access point.

- **Multi-Domain.** A single voice client and a single data client only can be authenticated and authorized on the interface before these clients are granted access to the interface. The voice and data domains are segregated. The RADIUS server attribute “Cisco-AVPair = ‘device-traffic-class = voice’” is used to identify a voice client.

For example, you can use this mode if an IP phone is connected to a NAS port and a laptop is connected to the hub port of the IP phone. Both devices need to be authenticated to access the network services behind the NAS.

- **Multi-Auth.** A single voice client and multiple data clients can be authenticated and authorized on the interface before these clients are granted access to the interface. The voice and data domains are segregated.

For example, you can use this mode if an IP phone and a network of computers are connected to a hub that is connected to a NAS port.

- **Multi-Domain-Multi-Host.** After one voice client and one data client are authenticated and authorized on the interface, access is granted to all clients that are connected to the interface, and all these clients are treated as data clients. The voice and data domains are segregated.

For example, you can use this mode if an IP phone is connected to a NAS port and a virtual machine controller (VMC) is connected to the hub port of the IP phone. Both the VMC and the IP phone need to be authenticated to access the
If the VMC hosts multiple virtual machines, after the VMC is authenticated, traffic is allowed from all virtual machines that are hosted by the VMC.

**Note:** If a data client is authenticated first, a voice client can be authenticated only through 802.1x.

**Note:** If the switch exceeds the limit of one hundred and four (104) 802.1x users, each interface can authenticate one additional voice client. (The limit of 104 clients can include MAB clients.) For example, even if the switch already supports 104 clients, each interface can still authenticate one additional IP phone.

- **Guest VLAN ID.** Specify the VLAN ID for the guest VLAN. The range is from 0 to 4093. The default value is 0. Enter 0 to reset the guest VLAN ID on the interface. The guest VLAN allows the port to provide a distinguished service to unauthenticated users, after three authentication failures. This feature provides a mechanism to allow users access to hosts on the guest VLAN.

- **Unauthenticated VLAN ID.** Specify the VLAN ID of the unauthenticated VLAN for the selected port. The range is from 0 to 3965. The default value is 0. Hosts that fail the authentication might be denied access to the network or placed on a VLAN created for unauthenticated clients. This VLAN might be configured with limited network access.

- **Periodic Reauthentication.** To allow periodic reauthentication of the supplicant for the specified port, select **Enable**

- **Reauthentication Period Type.** If you enable period authentication, select the type of reauthentication:
  - **Server.** The reauthentication time-out value from the server is used. This is the default setting. The server’s session time-out and session termination settings are used by the authenticator to reauthenticate a supplicant on the interface. An example of a server is a RADIUS server.
  - **User.** You must enter the time-out value in the **Reauthentication Period** field.

- **Reauthentication Period.** If you enable period authentication and you select **User** as the reauthentication period type, specify the time in seconds after which reauthentication of the supplicant occurs. The reauthentication period must be a value in the range from 1 to 65535 seconds. The default value is 3600 seconds.

- **Max ReAuth Requests.** Specify the maximum number of reauthentication requests for the port.

- **Quiet Period.** Specify the time in seconds that the port remains in the quiet state following a failed authentication exchange. While in the quite state, the port does not attempt to acquire a supplicant.

- **Resending EAP.** Specify the EAP retransmit period for the selected port. The transmit period is the time in seconds, after which an EAPoL EAP Request/Identify frame is resent to the supplicant.
• **MAX EAP Requests.** Specify the maximum number of EAP requests for the port. The value is the maximum number of times an EAPoL EAP Request/Identity message is retransmitted before the supplicant times out.

• **Supplicant Timeout.** Specify the supplicant time-out for the port. The supplicant time-out is the time in seconds after which the supplicant times out.

• **Server Timeout.** Specify the time that elapses before the switch resends a request to the authentication server.

8. Click the **Apply** button.
   
   Your settings are saved.

The following table describes the port authentication status information available on the page.

**Table 56. Port authentication status information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Direction</td>
<td>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).</td>
</tr>
<tr>
<td>PAE Capabilities</td>
<td>The port access entity (PAE) functionality of the selected port. The option is Authenticator or Supplicant.</td>
</tr>
</tbody>
</table>

Initialize 802.1X on a Port

**To initialize 802.1X on a port:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.

   The System Information page displays.

5. Select **Security > Port Authentication > Advanced > Port Authentication**.
   
   The Port Authentication page displays.

6. Select the check box associated with the port to initialize.

7. Click the **Initialize** button.
802.1X on the selected interface is reset to the initialization state. Traffic sent to and from the port is blocked during the authentication process. This button is available only if the control mode is auto. When you click this button, the action is immediate. You do not need to click the Apply button for the action to occur.

View the Port Summary

You can view summary information about the port-based authentication settings for each port.

To view the port summary:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

The following table describes the fields on the Port Summary page.

### Table 57. Port summary

<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>This field indicates the configured control mode for the port. The options are as follows:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Force Unauthorized.</strong> The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Force Authorized.</strong> The authenticator PAE unconditionally sets the controlled port to authorized.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Auto.</strong> The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>MAC Based.</strong> The authenticator PAE sets the controlled port mode to reflect the outcome of authentication exchanges between a supplicant, an authenticator, and an authentication server on a per supplicant basis.</td>
</tr>
<tr>
<td>Operating Control Mode</td>
<td>The control mode under which the port is actually operating. The options are as follows:</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>- MAC Based</td>
</tr>
<tr>
<td></td>
<td>- N/A: If the port is in detached state, it cannot participate in port access control.</td>
</tr>
<tr>
<td>Reauthentication Enabled</td>
<td>This field shows whether reauthentication of the supplicant for the specified port is allowed. The option is True or False. If the value is True, reauthentication occurs. Otherwise, reauthentication is not allowed.</td>
</tr>
<tr>
<td>Port Status</td>
<td>The authorization status of the specified port. The options are Authorized, Unauthorized, and N/A. If the port is in detached state, the value is N/A because the port cannot participate in port access control.</td>
</tr>
</tbody>
</table>

### View the Client Summary

You can display information about supplicant devices that are connected to the local authenticator ports. If no active 802.1X sessions exist, the table is empty.

**To view the client summary:**

1. Connect your computer to the same network as the switch.  
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.  
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **Security > Port Authentication > Advanced > Client Summary**.

The following table describes the fields on the Client Summary page.

**Table 58. Client Summary information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port to be displayed.</td>
</tr>
<tr>
<td>User Name</td>
<td>The user name representing the identity of the supplicant device.</td>
</tr>
<tr>
<td>Supplicant Mac Address</td>
<td>The supplicant’s device MAC address.</td>
</tr>
<tr>
<td>Session Time</td>
<td>The time since the supplicant logged in seconds.</td>
</tr>
<tr>
<td>Filter ID</td>
<td>The policy filter ID assigned by the authenticator to the supplicant device.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID assigned by the authenticator to the supplicant device.</td>
</tr>
<tr>
<td>VLAN Assigned</td>
<td>The reason for the VLAN ID assigned by the authenticator to the supplicant device.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>The session time-out imposed by the RADIUS server on the supplicant device.</td>
</tr>
<tr>
<td>Termination Action</td>
<td>The termination action imposed by the RADIUS server on the supplicant device.</td>
</tr>
</tbody>
</table>
Set Up Traffic Control

You can configure MAC filters, storm control, port security, and protected port settings.

Manage MAC Filtering

You can create MAC filters that limit the traffic allowed into and out of specified ports on the switch.

Create a MAC Filter

If a packet with a MAC address and VLAN ID that you specify for a filter is received on a port that is not part of the inbound filter, the packet is dropped.

A packet with a MAC address and VLAN ID that you specify for a filter can be transmitted only from a port that is part of the outbound filter.

To create a MAC filter:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.
   
   The System Information page displays.

The previous figure shows the MAC Filter Configuration page for models GS324T and GS324TP.

6. From the **MAC Filter** menu, select **Create Filter**.

   If you did not configure any filters, this is the only option available.

7. From the **VLAN ID** menu, select the VLAN that must be used with the MAC address.

8. In the **MAC Address** field, specify the MAC address of the filter in the format XX:XX:XX:XX:XX:XX.

   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

9. In the Port and LAG tables in the Source Port Members section, select the ports and LAGs that must be included in the inbound filter.

   If a packet with the MAC address and VLAN ID that you specify is received on a port that is not part of the inbound filter, the packet is dropped.

10. In the Port and LAG tables in the Destination Port Members section, select the ports and LAGs that must be included in the outbound filter.
A packet with the MAC address and VLAN ID that you specify can be transmitted only from a port that is part of the outbound filter.

**Note:** Destination ports can be included only in a multicast filter. A multicast filter is determined by the MAC address that you enter in the MAC Address field.

11. Click the **Apply** button.
   
   Your settings are saved.

Delete a MAC Filter

**To delete a MAC filter:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.
   
   The System Information page displays.

5. Select **Security > Traffic Control > MAC Filter > MAC Filter Configuration**.
   
   The MAC Filter Configuration page displays.

6. From the **MAC Filter** menu, select the filter.

7. Click the **Delete** button.
   
   The filter is removed.

MAC Filter Summary

You can view the MAC filters that are configured on the switch.

**To view the MAC filter summary:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
   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>The MAC address of the filter in the format XX:XX:XX:XX:XX:XX.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID used with the MAC address to fully identify packets you want filtered.</td>
</tr>
<tr>
<td>Source Port Members</td>
<td>The ports to be used for filtering inbound packets.</td>
</tr>
<tr>
<td>Destination Port Members</td>
<td>The ports to be used for filtering outbound packets.</td>
</tr>
</tbody>
</table>

Configure Storm Control Settings

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, cause the network to time out, or do both.

The switch measures the incoming packet rate per port for broadcast, multicast, unknown, and unicast packets and discards packets if the rate exceeds the defined value. You enable storm control per interface, by defining the packet type and the rate at which the packets are transmitted.

Configure Global Storm Control Settings

The global storm control settings apply to all ports. After you configure the global settings, you can specify storm control settings for one or more ports.
To configure global storm control settings:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.
   
   The System Information page displays.

5. Select Security > Traffic Control > Storm Control.

6. In the Storm Control section, from the Ingress Control Mode menu, select one of the following modes for storm control:
   
   - **Disabled.** Storm control is disabled. This is the default setting.
   
   - **Unknown Unicast.** If the rate of incoming unknown Layer 2 unicast traffic (that is, traffic for which a destination lookup failure occurs) increases beyond the configured threshold on an interface, the traffic is dropped.
   
   - **Multicast.** If the rate of incoming Layer 2 multicast traffic increases beyond the configured threshold on an interface, the traffic is dropped.
   
   - **Broadcast.** If the rate of incoming Layer 2 broadcast traffic increases beyond the configured threshold on an interface, the traffic is dropped.

7. If the selection from the Ingress Control Mode menu is not Disabled, specify whether the ingress control mode is enabled by selecting Enable or Disable from the Status menu.

8. 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 and 100%. The default is 5%.

9. From the **Control Action** mode menu, select one of the following options:
   - **None**. No action is taken. This is the default setting.
   - **Trap**. If the threshold of the configured broadcast storm is exceeded, a trap is sent.
   - **Shutdown**. If the threshold of the configured broadcast storm is exceeded, the port is shut down.

10. Click the **Apply** button.
    
    Your settings are saved.

Configure Storm Control Settings for One or More Ports

After you configure the global settings, you can specify storm control settings for one or more ports.

**To configure storm control settings for one or more ports:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#).
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.
   
   The System Information page displays.

5. Select **Security > Traffic Control > Storm Control**.
The default settings in the Port Settings section depends on the global storm control settings (see Configure Global Storm Control Settings on page 252), which apply to all ports.

6. In the Port Settings section, select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.

7. From the Status menu, specify whether the ingress control mode is enabled for the port by selecting Enable or Disable.

8. In the Threshold field, specify the maximum rate at which unknown packets are forwarded for the port.
   The range is a percent of the total threshold between 0 and 100%. The default is 5%.

9. From the Control Action mode menu, select one of the following options for the port:
   - None. No action is taken.
   - Trap. If the threshold of the configured broadcast storm is exceeded, a trap is sent.
   - Shutdown. If the threshold of the configured broadcast storm is exceeded, the port is shut down.

10. Click the Apply button.
    Your settings are saved.
Manage Port Security

Port security lets you lock one or more ports on the switch. When a port is locked, the port can only forward packets with a source MAC addresses that you specifically allowed. The port discards all other packets.

Configure the Global Port Security Mode

To configure the global port security mode:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.
   
   The System Information page displays.

   
   The Port Security Configuration page displays.
   
   The page also shows the Port Security Violations table.

6. To enable port security on the switch, select the Port Security Mode Enable radio button.
   
   The default is Disable.

7. Click the Apply button.
   
   Your settings are saved.
   
   By default, port security is disabled for individual ports.

8. After you enable port security for individual ports (see Configure a Port Security Interface on page 257), click the Refresh button to refresh the page with the latest information about the ports.
   
   The Port Security Violations 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 Violations table.

Table 60. Port Security Violations information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The physical interface.</td>
</tr>
<tr>
<td>Last Violation MAC</td>
<td>The source MAC address of the last packet that was discarded at a locked port.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID corresponding to the last MAC address violation.</td>
</tr>
</tbody>
</table>

Configure a Port Security Interface

A MAC address can be defined as allowed on a port by one of two methods: dynamically or statically. Both methods can be 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 is not reached, a packet with an unknown source MAC address is learned and forwarded normally. If the limit is reached, no more addresses are learned on the port. Any packets with source MAC addresses that were not already learned are dropped. 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 configure a port security interface:

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   - The login window opens.

4. Enter the switch’s password in the Password field.
   - The default password is password.
   - The System Information page displays.

6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   • **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   • **LAG**. Only LAGs are displayed.
   • **All**. Both physical interfaces and LAGs are displayed.

7. Select one or more interfaces by taking one of the following actions:
   • To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   • To configure multiple interfaces with the same settings, select the check box associated with each interface.
   • To configure all interfaces with the same settings, select the check box in the heading row.

8. Specify the following settings:
   • **Port Security**. Enable or disable the port security feature for the selected interfaces. The default is Disable.
   • **Max Learned MAC Address**. Specify the maximum number of dynamically learned MAC addresses on the selected interfaces. The default is 4096.
   • **Max Static MAC Address**. Specify the maximum number of statically locked MAC addresses on the selected interfaces. The default is 48.
   • **Enable Violation Shutdown**. Enable or disable shutdown of the selected interfaces if a packet with a disallowed MAC address is received. The default value is No, which means that the option is disabled.
   • **Enable Violation Traps**. Enable or disable the sending of new violation traps if a packet with a disallowed MAC address is received. The default value is No, which means that the option is disabled.

9. Click the **Apply** button.
   Your settings are saved.
View Learned MAC Addresses and Convert Them to Static MAC Addresses

After you enabled port security globally (see Configure the Global Port Security Mode on page 256) and enabled port security for specific interfaces (see Configure a Port Security Interface on page 257), you can convert a dynamically learned MAC address to a statically locked address.

To view learned MAC addresses for an individual interface or LAG and convert these MAC addresses to static MAC addresses:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.


6. From the Port List menu, select the individual interface.
   Port security must be enabled on the selected interface.

   The Dynamic MAC Address Table displays the MAC addresses and their associated VLANs that were learned on the selected port.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID corresponding to the MAC address.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC addresses learned on a specific port.</td>
</tr>
</tbody>
</table>
7. To convert the dynamically learned MAC address to a statically locked addresses, select the **Convert Dynamic Address to Static** check box.

8. Click the **Apply** button.

   The dynamic MAC address entries are converted to static MAC address entries in a numerically ascending order until the static limit is reached.

   The Number of Dynamic MAC Addresses Learned field displays the number of dynamically learned MAC addresses on a specific port.

9. To refresh the page with the latest information about the switch, click the **Refresh** button.

**Configure Protected Ports**

If you configure a port as protected, it does not forward traffic to any other protected port on the switch, but it does forward traffic to unprotected ports. You can configure the ports as protected or unprotected.

**To configure protected ports:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.

   The login window opens.

4. Enter the switch’s password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Traffic Control > Protected Port**.

   ![Protected Ports Membership](image)

   The previous figure shows the Protected Ports Membership page for models GS324T and GS324TP.

6. In the Ports table, click each port that you want to configure as a protected port.
Protected ports are marked with a check mark. No traffic forwarding is possible between two protected ports.

7. Click the **Apply** button.

Your settings are saved.

## Configure Access Control Lists

Access control lists (ACLs) ensure that only authorized users can access specific resources while blocking any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents, decide which types of traffic are forwarded or blocked, and provide security for the network. You can configure IPv4 and MAC ACLs.

**To configure an ACL:**

1. Create an IPv4-based or MAC-based ACL ID.
2. Create a rule and assign it to a unique ACL ID.
3. Define the rules, which can identify protocols, source, and destination IP and MAC addresses, and other packet-matching criteria.
4. Use the ID number to assign the ACL to a port or to a LAG.

To view ACL configuration examples, see [Access Control Lists (ACLs)](on page 340).

### Use the ACL Wizard to Create a Simple ACL

The ACL Wizard helps you create a simple ACL and apply it to the selected ports easily and quickly. First, select an ACL type to use when you create an ACL. Then add an ACL rule to this ACL and apply this ACL on the selected ports. The ACL Wizard allows you to create the ACL, but does not allow you to modify it. To modify the ACL, go to the ACL Configuration page. See [Configure a Basic or Extended IP ACL](on page 275).

---

**Note:** The steps in the following procedure describe how you can create an ACL based on the destination MAC address. If you select a different type of ACL (or example, an ACL based on a source IPv4), the page displays different information.

---

**To use the ACL Wizard to create an ACL:**

1. Connect your computer to the same network as the switch.

You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
5. Select Security > ACL > ACL Wizard.

The previous figure shows the ACL Wizard page for models GS324T and GS324TP.
6. From the ACL Type menu, select the type of ACL.
   You can select from the following ACL types:
   - **ACL Based on Destination MAC**. Creates an ACL based on the destination MAC address, destination MAC mask, and VLAN.
   - **ACL Based on Source MAC**. Creates an ACL based on the source MAC address, source MAC mask, and VLAN.
   - **ACL Based on Destination IPv4**. Creates an ACL based on the destination IPv4 address and IPv4 address mask.
   - **ACL Based on Source IPv4**. Creates an ACL based on the source IPv4 address and IPv4 address mask.
   - **ACL Based on Destination IPv4 L4 Port**. Creates an ACL based on the destination IPv4 Layer 4 port number.
   - **ACL Based on Source IPv4 L4 Port**. Creates an ACL based on the source IPv4 Layer 4 port number.
**Note:** For L4 port options, two rules are created (one for TCP and one for UDP).

7. In the **Sequence Number** field, enter a whole number in the range from 1 to 2147483647 that is used to identify the rule.

8. From the **Action** menu, select **Permit** or **Deny** to specify the action that must be taken if a packet matches the rule's criteria.

9. From the **Match Every** menu, select one of the following options:
   - **False.** Packets do not need to match the selected ACL and rule. With this selection, you can add a destination MAC address, destination MAC mask, and VLAN.
   - **True.** All packets must match the selected ACL and rule and are either permitted or denied. In this case, since all packets match the rule, the option of configuring other match criteria is not offered.

10. Specify the additional match criteria for the selected ACL type.

The rest of the rule match criteria fields available for configuration depend on the selected ACL type. For information about the possible match criteria fields, see the following table.

<table>
<thead>
<tr>
<th>ACL Based On</th>
<th>Fields</th>
</tr>
</thead>
</table>
| Destination MAC    | • **Destination MAC.** Specify the destination MAC address to compare against an Ethernet frame. The format is xx:xx:xx:xx:xx:xx. The BPDU keyword might be specified using a destination MAC address of 01:80:C2:xx:xx:xx.  
  • **Destination MAC Mask.** Specify the destination MAC address mask, which represents the bits in the destination MAC address to compare against an Ethernet frame. The format is xx:xx:xx:xx:xx:xx. The BPDU keyword might be specified using a destination MAC mask of 00:00:00:ff:ff:ff.  
  • **VLAN.** Specify the VLAN ID to match within the Ethernet frame. |
| Source MAC         | • **Source MAC.** Specify the source MAC address to compare against an Ethernet frame. The format is xx:xx:xx:xx:xx:xx.  
  • **Source MAC Mask.** Specify the source MAC address mask, which represents the bits in the source MAC address to compare against an Ethernet frame. The format is (xx:xx:xx:xx:xx:xx).  
  • **VLAN.** Specify the VLAN ID to match within the Ethernet frame. |
| Destination IPv4   | • **Destination IP Address.** Specify the destination IP address.  
  • **Destination IP Mask.** Specify the destination IP address mask. |
| Source IPv4        | • **Source IP Address.** Specify the source IP address.  
  • **Source IP Mask.** Specify the source IP address mask. |
| Destination IPv4 L4 Port | • **Destination L4 port (Protocol).** Specify the destination IPv4 L4 port protocol.  
  • **Destination L4 port (Value).** Specify the destination IPv4 L4 port value. |
| Source IPv4 L4 Port | • **Source L4 port (Protocol).** Specify the source IPv4 L4 port protocol.  
  • **Source L4 port (Value).** Specify the source IPv4 L4 port value. |
As a sample, the following steps describe how you can specify the additional match criteria for an ACL based on the destination MAC address:

a. In the **Destination MAC** field, specify the destination MAC address that must be compared against the information in an Ethernet frame.
   

b. In the **Destination MAC Mask** field, specify the destination MAC address mask that must be compared against the information in an Ethernet frame.
   
   The format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC mask of 00:00:00:ff:ff:ff.

c. In the **VLAN ID** field, specify which VLAN must be compared against the information in an Ethernet frame.
   
   The range is from 1 to 4093. Either a VLAN range or VLAN can be configured.

11. In the Binding Configuration section, from the **Direction** menu, select the packet filtering direction for the ACL.
   
   Only the inbound direction is valid.

12. In the Ports and LAG tables in the Binding Configuration section, select the ports and LAGs to which the ACL must be applied.

13. Click the **Add** button.
   
   The rule is added to the ACL.

14. Click the **Apply** button.
   
   Your settings are saved.

Modify an ACL Rule

**To modify an ACL rule:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.

   The login window opens.

4. Enter the switch’s password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Security > ACL > ACL Wizard**.
   The ACL Wizard page displays.

6. Select check box that is associated with the rule.

7. Update the match criteria as needed.

8. Click the **Apply** button.
   Your settings are saved.

Delete an ACL Rule

**To delete an ACL rule:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address** on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **Security > ACL > ACL Wizard**.
   The ACL Wizard page displays.

6. Select check box that is associated with the rule.

7. Click the **Delete** button.
   The rule is removed.

ACL Wizard Example

In the following figure, the ACL rule is configured to check for packet matches on ports 4, 5, 18, and 19 and on LAG 1. Only the Inbound option is valid. Packets that include a source address in the 192.168.5.0/16 network and VLAN 22 are permitted to be forwarded by the interfaces. All other packets are dropped because every ACL includes an implicit **deny all** rule as the last rule.
The previous figure shows a sample for models GS324T and GS324TP.

For information about the ACL Wizard, see Use the ACL Wizard to Create a Simple ACL on page 261.

Configure a Basic MAC ACL

A MAC ACL consists of a set of rules that are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit or Deny) is taken, and the additional rules are not checked for a match.

Multiple steps are involved in defining a MAC ACL and applying it to the switch:

1. Create a MAC ACL ID (see Add a MAC ACL on page 266).
2. Create a MAC rule (see Configure MAC ACL Rules on page 268).
3. Associate the MAC ACL with one or more interfaces (see Configure MAC Bindings on page 272).

You can view or delete MAC ACL configurations in the MAC Binding table (see View or Delete MAC ACL Bindings in the MAC Binding Table on page 274).

Add a MAC ACL

To add a MAC ACL:

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.

The System Information page displays.

5. Select **Security > ACL > Basic > MAC ACL**.

   ![MAC ACL Table](image)

   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 plus the number of configured MAC ACLs.

6. In the **Name** field, specify a name for the MAC ACL.
   The name string can include alphabetic, numeric, hyphen, underscore, or space characters only. The name must start with an alphabetic character.

7. Click the **Add** button.
   The MAC ACL is added.

   Each configured ACL displays the following information:
   - **Rules**: The number of rules currently configured for the MAC ACL.
   - **Direction**: The direction of packet traffic affected by the MAC ACL, which can be Inbound or blank. (If the ACL is not bound to an interface, the direction is blank.)

**Change the Name of a MAC ACL**

**To change the name of a MAC ACL:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is *password*.
   The System Information page displays.

5. Select **Security > ACL > Basic > MAC ACL**.
   The MAC ACL page displays.

6. Select check box that is associated with the MAC ACL.

7. In the **Name** field, specify the new name.

8. Click the **Apply** button.
   Your settings are saved.

**Delete a MAC ACL**

**To delete a MAC ACL:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is *password*.
   The System Information page displays.

5. Select **Security > ACL > Basic > MAC ACL**.
   The MAC ACL page displays.

6. Select check box that is associated with the MAC ACL.

7. Click the **Delete** button.
   The MAC ACL is removed.

**Configure MAC ACL Rules**

You can 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.
Add a Rule to a MAC ACL

To add a rule to a MAC ACL:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch. If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12. The login window opens.

4. Enter the switch’s password in the Password field. The default password is password. The System Information page displays.

5. Select Security > ACL > Basic > MAC Rules.

6. From the ACL Name menu, select the MAC ACL.

7. In the Sequence Number field, enter a whole number in the range from 1 to 2147483647 to identify the rule.

8. From the Action menu, select the action that must 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.

9. In the Assign Queue field, specify the hardware egress queue identifier that must be used to handle all packets matching this ACL rule.
   For models GS324T and GS324TP, the range for the queue ID is from 0 to 3. For model GS348T, the range for the queue ID is from 0 to 7.

10. From the Mirror Interface menu, select the specific egress interface to which the matching traffic stream must be copied, in addition to being forwarded normally by the switch.
This field cannot be set if a redirect interface is already configured for the ACL rule. This field is visible for a Permit action.

11. From the **Redirect Interface** menu, select the egress interface to which the matching traffic stream must be redirected, bypassing any forwarding decision normally performed by the switch.

   This field cannot be set if a mirror interface is already configured for the ACL rule.

12. From the **Match Every** menu, select whether each Layer 2 MAC packet must be matched against the rule:
   - **True**. Each packet must match the selected ACL rule.
   - **False**. Not all packets need to match the selected ACL rule.

13. In the **CoS** field, specify the 802.1p user priority that must be compared against the information in an Ethernet frame.

   The range for the priority is from 0 to 7.

14. In the **Destination MAC** field, specify the destination MAC address that must be compared against the information in an Ethernet frame.


15. In the **Destination MAC Mask** field, specify the destination MAC address mask that must be compared against the information in an Ethernet frame.

   The format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC mask of 00:00:00:ff:ff:ff.

16. From the **EtherType Key** menu, select the EtherType value that must be compared against the information in an Ethernet frame.

   The values are as follows:
   - **Apple Talk**
   - **IBM SNA**
   - **IPv4**
   - **IPv6**
   - **IPX**
   - **MPLS Multicast**
   - **MPLS Unicast**
   - **NetBios**
   - **Novell**
   - **PPPOE**
   - **RARP**
   - **User Value**

17. If you select **User Value** from the **EtherType Key** menu, in the **EtherType User Value** field, specify the customized EtherType value that must be used.
This value must be compared against the information in an Ethernet frame. The range is from 0x0600 to 0xFFFF.

18. In the **Source MAC** field, specify the source MAC address that must be compared against the information in an Ethernet frame.


19. In the **Source MAC Mask** field, specify the source MAC address mask that must be compared against the information in an Ethernet frame.


20. In the **VLAN** field, specify the VLAN ID that must be compared against the information in an Ethernet frame.

   The range is from 1 to 4093. Either VLAN range or VLAN can be configured.

21. If the selection from the **Action** menu is **Deny**, from the **Logging** menu, select whether to enable or disable logging.

   If you select **Enable**, logging is enabled for this ACL rule (subject to resource availability on the switch).

   **Note:** If you enable logging and you also enable ACL system traps (see **Configure SNMPv1/v2 Trap Flags** on page 82), a SNMP trap is sent when a packet matches this ACL rule.

22. Click the **Add** button.

    The rule is added.

**Change the Match Criteria for a MAC Rule**

**To change the match criteria for a MAC rule:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address** on page 12.

   The login window opens.

4. Enter the switch’s password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Basic > MAC Rules**.

   The MAC Rules page displays.
6. Select the check box that is associated with the rule.
7. Modify the fields as needed.
8. Click the **Apply** button.
   Your settings are saved.

#### Delete a Rule for a MAC ACL

**To delete a rule for a MAC:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the **Password** field.
   The default password is `password`.
   The System Information page displays.
5. Select **Security > ACL > Basic > MAC Rules**.
   The MAC Rules page displays.
6. Select the check box that is associated with the rule.
7. Click the **Delete** button.
   The rule is removed.

#### Configure MAC Bindings

When an ACL is bound to an interface, all the rules that are defined are applied to the selected interface. You can assign MAC ACLs lists to interfaces and LAGs.

**To configure MAC bindings:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.

   The System Information page displays.


   The previous figure shows the MAC Binding Configuration page for models GS324T and GS324TP. The figure shows two MAC ACL examples in the table.

   6. From the ACL ID menu, select an ACL.
      The fixed selection from the Direction menu is Inbound, which means that MAC ACL rules are applied to traffic entering the interface.

   7. In the Sequence Number field, optionally specify a number to indicate the order of the access list relative to other access lists already assigned to the interface and direction.
      A low number indicates high precedence order. If a sequence number is already in use for the interface and direction, the specified access list replaces the currently attached access list using that sequence number. If you do not specify the sequence number, a sequence number that is one number greater than the highest sequence number currently in use for the interface and direction is used. The range is from 1 to 4294967295.

   8. To add the selected ACL to a port or LAG, in the Ports table or LAG table, click the port or LAG so that a check mark displays.
      You can add the ACL to several ports and LAGs.
The Ports and LAG tables display the available interfaces for ACL bindings. All nonrouting physical interfaces, VLAN interfaces, and interfaces participating in LAGs are listed.

9. Click the **Apply** button.

Your settings are saved.

The following table describes the information displayed in the Interface Binding Status table.

**Table 61. Interface Binding Status table**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface of the ACL assigned.</td>
</tr>
<tr>
<td>Direction</td>
<td>The selected packet filtering direction for the ACL.</td>
</tr>
<tr>
<td>ACL Type</td>
<td>The type of ACL assigned to the selected interface and direction.</td>
</tr>
<tr>
<td>ACL ID</td>
<td>The ACL name identifying the ACL assigned to the selected interface and direction.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.</td>
</tr>
</tbody>
</table>

**View or Delete MAC ACL Bindings in the MAC Binding Table**

You can view or delete the MAC ACL bindings in the MAC Binding Table.

**To view or delete MAC ACL bindings:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address on page 12**.
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.
   
   The System Information page displays.

5. Select **Security > ACL > Basic > MAC Binding Table**.
6. To delete a MAC ACL-to-interface binding, do the following:
   a. Select the check box next to the interface.
   b. Click the Delete button.

   The binding is removed.

The following table describes the information that is displayed in the MAC Binding Table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface of the ACL assigned.</td>
</tr>
<tr>
<td>Direction</td>
<td>The selected packet filtering direction for the ACL.</td>
</tr>
<tr>
<td>ACL Type</td>
<td>The type of ACL assigned to the selected interface and direction.</td>
</tr>
<tr>
<td>ACL ID</td>
<td>The ACL name identifying the ACL assigned to the selected interface and direction.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.</td>
</tr>
</tbody>
</table>

Configure a Basic or Extended IP ACL

An IP ACL consists of a set of rules that are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit or Deny) is taken, and the additional rules are not checked for a match. You must specify the interfaces to which an IP ACL applies, as well as whether it applies to inbound or outbound traffic.

Multiple steps are involved in defining an IP ACL and applying it to the switch:

1. Add an IP ACL ID (see Add an IP ACL on page 276).

   The differences between a basic IP ACL and an extended IP ACL are as follows:

   - **Numbered ACL from 1 to 99.** Creates a basic IP ACL, which allows you to permit or deny traffic from a source IP address.
   - **Numbered ACL from 100 to 199.** Creates an extended IP 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 basic IP ACL.
   - **Named IP ACL.** Create an extended IP ACL with a name string that is up to 31 alphanumeric characters in length. The name must start with an alphabetic character.

2. Create an IP rule (see Configure Rules for a Basic IP ACL on page 278 or Configure Rules for an Extended IP ACL on page 282).
3. Associate the IP ACL with one or more interfaces (see Configure IP ACL Interface Bindings on page 289).

You can view or delete IP ACL configurations in the IP ACL Binding table (see View or Delete IP ACL Bindings in the IP ACL Binding Table on page 291.

Add an IP ACL

To add an IP ACL:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.

   The System Information page displays.

5. Select Security > ACL > Advanced > IP ACL.

   The IP ACL page shows the current size of the ACL table compared to the maximum size of the ACL table. The current size is equal to the number of configured IPv4 ACLs plus the number of configured MAC ACLs. The maximum size is 100.

   The Current Number of ACL field displays the current number of all ACLs configured on the switch.

   The Maximum ACL field displays the maximum number of IP ACLs that can be configured on the switch.
6. In the **IP ACL ID** field, specify the ACL ID or IP ACL name, which depends on the IP ACL type. The IP ACL ID is an integer in the following range:
   - **1–99.** Creates a basic IP ACL, which allows you to permit or deny traffic from a source IP address.
   - **100–199.** Creates an extended IP 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.
   - **IP ACL Name.** Create an extended IP ACL with a name string that is up to 31 alphanumeric characters in length. The name must start with an alphabetic character.

Each configured ACL displays the following information:
   - **Rules.** The number of rules currently configured for the IP ACL.
   - **Type.** Identifies the ACL as a basic IP ACL (with ID from 1 to 99), extended IP ACL (with ID from 100 to 199 or a name).

7. Click the **Add** button.
   The IP ACL is added.

**Change the Name of an IP ACL**

**To change the name of an IP ACL:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **Security > ACL > Advanced > IP ACL.**
   The IP ACL Configuration page displays.

6. Select the check box that is associated with the IP ACL.

7. In the **IP ACL** field, specify the new name.

8. Click the **Apply** button.
   Your settings are saved.
Delete an IP ACL

**To delete an IP ACL:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.

   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Advanced > IP ACL**.

   The IP ACL Configuration page displays.

6. Select the check box that is associated with the IP ACL.

7. Click the **Delete** button.

   The IP ACL is removed.

---

**Configure Rules for a Basic IP ACL**

You can define rules for IP-based standard ACLs (basic ACLs). The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

---

**Note:** An implicit *deny all* rule is included 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.

---

**Add a Rule for a Basic IP ACL**

**To add a rule for a basic IP ACL:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

   ![IP Rules](image)

   If no rules exist, the Basic ACL Rule Table shows the message No rules have been configured for this ACL. If one or more rules exist for the ACL, the rules display in the Basic ACL Rule Table.

6. From the ACL ID menu, select the IP ACL for which you want to add a rule.
   For basic IP ACLs, this must be an ID in the range from 1 to 99.
7. Click the Add button.

   ![IP Rule Configuration](image)

   The previous figure shows the page for model GS348T.
8. Specify the following match criteria for the rule:
   • **Sequence Number.** Enter an ACL sequence number in the range from 1 to 2147483647 that is used to identify the rule. An IP ACL can contain up to 50 rules.
   • **Action.** Select the ACL forwarding action, which is one of the following:
     - **Permit.** Forward packets that meet the ACL criteria.
       - **Egress Queue.** If the selection form the **Action** menu is **Permit**, you can specify the hardware egress queue identifier that is used to handle all packets matching this IP ACL rule.
         For models GS324T and GS324TP, the range for the queue ID is from 0 to 3. For model GS348T, the range for the queue ID is from 0 to 7.
     - **Deny.** Drop packets that meet the ACL criteria.
       - **Logging.** If the selection from the **Action** menu is **Deny**, you can enable logging for the ACL by selecting the **Enable** radio button. (Logging is subject to resource availability on the switch.)
         If you enable logging and you also enable ACL system traps (see **Configure SNMPv1/v2 Trap Flags** on page 82), a SNMP trap is sent when a packet matches this ACL rule.
   • **Match Every.** Select one of the radio buttons to specify whether all packets must match the selected IP ACL rule:
     - **Enable.** All packets must match the selected IP ACL rule and are either permitted or denied.
     - **Disable.** Not all packets need to match the selected IP ACL rule.
   • **Interface.** Select one of the radio buttons to specify whether all packets must be mirrored or redirected:
     - **Mirror.** From the menu, select the specific egress interface to which the matching traffic stream must be copied, in addition to being forwarded normally by the switch.
     - **Redirect.** From the menu, select the egress interface to which the matching traffic stream must be redirected, bypassing any forwarding decision normally performed by the switch.
   • **Src IP Address.** Enter an IP address using dotted-decimal notation to be compared to a packet's source IP address as a match criterion for the selected IP ACL rule.
   • **Src IP Mask.** Specify the IP mask in dotted-decimal notation to be used with the source IP address value.

9. Click the **Apply** button.
   Your settings are saved.
Modify the Match Criteria for a Basic IP ACL Rule

To modify the match criteria for a basic IP ACL rule:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
   The IP Rules page displays.
6. From the ACL ID menu, select the ACL that includes the rule that you want to modify.
7. In the Basic ACL Rule Table, click the rule.
   The rule is a hyperlink. The Standard ACL Rule Configuration page displays.
8. Modify the basic IP ACL rule criteria.
9. Click the Apply button.
   Your settings are saved.

Delete a Basic IP ACL Rule

To delete a basic IP ACL rule:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
The System Information page displays.

   The IP Rules page displays.

6. From the ACL ID menu, select the ACL that includes the rule that you want to modify.

7. In the Basic ACL Rule Table, select the check box that is associated with the rule.

8. Click the Delete button.
   The rule is removed.

Configure Rules for an Extended IP ACL

You can define rules for extended IP-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

---

**Note:** An implicit *deny all* rule is included 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.

---

Add a Rule for an Extended IP ACL

**To add a rule for an extended IP ACL:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is **password**.
   The System Information page displays.

The previous figure does not show all columns on the page.

If no rules exist, the Extended ACL Rule Table shows the message *No rules have been configured for this ACL*. If one or more rules exist for the ACL, the rules display in the Extended ACL Rule Table.

6. From the **ACL ID** menu, select the IP ACL for which you want to add a rule.

   For extended IP ACLs, this must be an ID in the range from 101 to 199 or a name.

7. Click the **Add** button.

The previous figure shows the page for model GS348T.

8. Configure the following match criteria for the rule:
   - **Sequence Number**: Enter a number in the range from 1 to 2147483647 that is used to identify the rule. An extended IP ACL can contain up to 50 rules.
   - **Action**: Select the ACL forwarding action, which is one of the following:
     - **Permit**: Forward packets that meet the ACL criteria.
     - **Deny**: Drop packets that meet the ACL criteria.
   
   **Egress Queue**: If the selection from the **Action** menu is **Permit**, select the hardware egress queue identifier that is used to handle all packets matching this IP ACL rule.
For models GS324T and GS324TP, the range for the queue ID is from 0 to 3. For model GS348T, the range for the queue ID is from 0 to 7.

- **Deny.** Drop packets that meet the ACL criteria.

**Logging.** If the selection from the Action menu is Deny, you can enable logging for the ACL by selecting the Enable radio button. (Logging is subject to resource availability in the device.)

If you enable logging and you also enable ACL system traps (see Configure SNMPv1/v2 Trap Flags on page 82), a SNMP trap is sent when a packet matches this ACL rule.

- **Interface.** For a Permit action, use either a mirror interface or a redirect interface:
  - Select the Mirror radio button and use the menu to specify the egress interface to which the matching traffic stream is copied, in addition to being forwarded normally by the device.
  - Select the Redirect radio button and use the menu to specify the egress interface to which the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device.

- **Match Every.** Select one of the radio buttons to specify whether all packets must match the selected IP ACL rule:
  - **False.** Not all packets need to match the selected IP ACL rule. You can configure other match criteria on the page.
  - **True.** All packets must match the selected IP ACL rule and are either permitted or denied. In this case, you cannot configure other match criteria on the page.

- **Protocol Type.** From the menu, select a protocol that a packet’s IP protocol must be matched against: IP, ICMP, IGMP, TCP, UDP, EIGRP, GRE, IPINIP, OSPF, PIM, or Other. If you select Other, enter a protocol number from 0 to 255.

- **Src.** In the Src field, enter a source IP address, using dotted-decimal notation, to be compared to a packet’s source IP address as a match criterion for the selected IP ACL rule:
  - If you select the IP Address radio button, enter an IP address or an IP address range. You can enter a relevant wildcard mask to apply this criteria. If this field is left empty, it means any.
  - If you select the Host radio button, the wildcard mask is configured as 0.0.0.0. If this field is left empty, it means any.

The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that none of the bits are important. A wildcard of 255.255.255.255 indicates that all of the bits are important.

- **Src L4.** The options are available only when the protocol is set to TCP or UDP. Use the source L4 port option to specify relevant matching conditions for L4 port numbers in the extended ACL rule.
You can select either the **Port** radio button or the **Range** radio button:

- **Port.** If you select the **Port** radio button, you can either enter the port number yourself or select one of the following protocols from the menu:
  
  - The source IP TCP port protocols are **Domain**, **Echo**, **FTP**, **FTP data**, 
  
  - The source IP UDP port protocols are **Domain**, **Echo**, **SNMP**, **NTP**, **RIP**, **Time**, 
    **Who**, and **TFTP**.

  Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

  Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.

  The relevant matching conditions for L4 port numbers are as follows:

  - **Equal.** IP ACL rule matches only if the Layer 4 source port number is equal to the specified port number or port protocol.
  
  - **Less Than.** IP ACL rule matches if the Layer 4 source port number is less than the specified port number.
  
  - **Greater Than.** IP ACL rule matches if the Layer 4 source port number is greater than the specified port number.
  
  - **Not Equal.** IP ACL rule matches only if the Layer 4 source port number is not equal to the specified port number or port protocol.

- **Range.** If you select the **Range** radio button, the IP ACL rule matches only if the Layer 4 source port number is within the specified port range. The starting port, ending port, and all ports in between are a part of the Layer 4 port range.

  The **Start Port** and **End Port** fields identify the first and last ports that are part of the port range. The values can range from 0 to 65535.

  You can either enter the port range yourself or select one of the following protocols from the menu:

  - The source IP TCP port range names are **Domain**, **Echo**, **FTP**, **FTP data**, 
  
  - The source IP UDP port range names are **Domain**, **Echo**, **SNMP**, **NTP**, **RIP**, 
    **Time**, **Who**, and **TFTP**.

  Each of these values translates into its equivalent port number, which is used as both the start and end of the port range. Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.

  The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard of 255.255.255.255 indicates that *all* of the bits are important.
• **Dst.** In the **Dst** field, enter a destination IP address, using dotted-decimal notation, to be compared to a packet's destination IP address as a match criterion for the selected IP ACL rule:
  - If you select the **IP Address** radio button, enter an IP address with a relevant wildcard mask to apply this criteria. If this field is left empty, it means *any*.
  - If you select the **Host** radio button, the wildcard mask is configured as 0.0.0.0. If this field is left empty, it means *any*.

The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard of 255.255.255.255 indicates that *all* of the bits are important.

• **Dst L4.** The options are available only when the protocol is set to TCP or UDP. Use the destination L4 port option to specify relevant matching conditions for L4 port numbers in the extended ACL rule.

You can select either the **Port** radio button or the **Range** radio button:

- **Port.** If you select the **Port** radio button, you can either enter the port number yourself or select one of the following protocols from the menu.
  - The destination IP UDP port protocols are **Domain**, **Echo**, **SNMP**, **NTP**, **RIP**, **Time**, **Who**, and **TFTP**.

Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.

The relevant matching conditions for L4 port numbers are as follows:

- **Equal.** The IP ACL rule matches only if the Layer 4 destination port number is equal to the specified port number or port protocol.
- **Less Than.** The IP ACL rule matches if the Layer 4 destination port number is less than the specified port number.
- **Greater Than.** The IP ACL rule matches if the Layer 4 destination port number is greater than the specified port number.
- **Not Equal.** The IP ACL rule matches only if the Layer 4 destination port number is not equal to the specified port number or port protocol.

- **Range.** If you select the **Range** radio button, the IP ACL rule matches only if the Layer 4 destination port number is within the specified port range. The starting port, ending port, and all ports in between are a part of the Layer 4 port range.

The **Start Port** and **End Port** fields identify the first and last ports that are part of the port range. They values can range from 0 to 65535.
You can either select the enter the port range yourself or select one of the following protocols from the menu:

- The destination IP TCP port range names are **Domain, Echo, FTP, FTP data, www-http, SMTP, Telnet, POP2, POP3, and bgp.**
- The destination IP UDP port range names are **Domain, Echo, SNMP, NTP, RIP, Time, Who, and TFTP.**

Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means **any.**

The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that **none** of the bits are important. A wildcard of 255.255.255.255 indicates that **all** of the bits are important.

- **IGMP Type.** If your selection from the **Protocol Type** menu is **IGMP** and you specify the IGMP type, the IP ACL rule matches the specified IGMP message type. The range is from 0 to 255. If this field is left empty, it means **any.**
- **ICMP.** If your selection from the **Protocol Type** menu is **ICMP**, you can select either the **Type** or **Message** radio button:
  - **Type.** If you select the **Type** radio button, note the following:
    - The **Type** and **Code** fields are enabled only if the protocol is ICMP. Use these fields to specify a match condition for ICMP packets:
    - If you specify information in the **Type** field, the IP ACL rule matches the specified ICMP message type. The type number can be from 0 to 255.
    - If you specify information in the **Code** field, the IP ACL rule matches the specified ICMP message code. The code can be from 0 to 255.
    - If these fields are left empty, it means **any.**
  - **Message.** If you select the **Message** radio button, from the menu, select the type of the ICMP message to match with the selected IP ACL rule. Specifying a type of message implies that both the ICMP type and ICMP code are specified. The ICMP message is decoded into the corresponding ICMP type and ICMP code within the ICMP type.

  The IPv4 ICMP message types are **Echo, echo-reply, host-redirect, mobile-redirect, net-redirect, net-unreachable, redirect, packet-too-big, port-unreachable, source-quench, router-solicitation, router-advertisement, TTL-exceeded, time-exceeded, and unreachable.**

- **Fragments.** Either select the **Enable** radio button to allow initial fragments (that is, the fragment bit is asserted) or leave the default **Disable** radio button selected to prevent initial fragments from being used.

  This option is not valid for rules that match L4 information such as a TCP port number, because that information is carried in the initial packet.

- **Service Type.** Select a service type match condition for the extended IP ACL rule.
The possible options are **IP DSCP**, **IP precedence**, and **IP TOS**, which are alternative methods to specify a match criterion for the same service type field in the IP header. Each method uses a different user notation. After you make a selection, you can specify the appropriate values:

- **IP DSCP.** This is an optional configuration. Specify the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order 6 bits of the service type octet in the IP header. Enter an integer from 0 to 63. To select the IP DSCP, select one of the DSCP keywords from the menu. To specify a numeric value, select Other and a field displays in which you can enter numeric value of the DSCP.

- **IP Precedence.** This is an optional configuration. The IP precedence field in a packet is defined as the high-order 3 bits of the service type octet in the IP header. Enter a number from 0 to 7.

- **IP TOS.** This is an optional configuration. The IP ToS field in a packet is defined as all 8 bits of the service type octet in the IP header. The ToS bits value is a hexadecimal number that is composed of numbers 00 to 09 and AA to FF. The ToS mask value is a hexadecimal number that is composed of numbers 00 to FF. The ToS mask denotes the bit positions in the ToS bits value that are used for comparison against the IP ToS field in a packet.

For example, to check for an IP ToS value for which bit 7 is set and is the most significant value, for which bit 5 is set, and for which bit 1 is cleared, use a ToS bits value of 0xA0 and a ToS mask of 0xFF.

9. Click the **Apply** button.

Your settings are saved.

Modify the Match Criteria for an Extended IP ACL Rule

**To modify the match criteria for an existing extended IP ACL rule:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address on page 12](#).

   The login window opens.

4. Enter the switch’s password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Advanced > IP Extended Rules**.

   The IP Rules page displays.
6. From the ACL ID menu, select the ACL that includes the rule that you want to modify.
7. In the Extended ACL Rule Table, click the rule.
   The rule is a hyperlink. The Extended ACL Rule Configuration page displays.
8. Modify the extended IP ACL rule criteria.
9. Click the Apply button.
   Your settings are saved.

Delete an Extended IP ACL Rule

To delete an extended IP ACL rule:
1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or
   connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP
   Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
   The IP Rules page displays.
6. From the ACL ID menu, select the ACL that includes the rule that you want to delete.
7. In the Extended ACL Rule Table, select the check box that is associated with the rule.
8. Click the Delete button.
   The rule is removed.

Configure IP ACL Interface Bindings

When you bind an IP ACL to an interface, all the rules that you defined for the IP ACL are
applied to the selected interface.
If resources on the switch are insufficient, an attempt to bind an ACL to an interface fails.
To bind an IP ACL to one or more interfaces:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.


   The previous figure shows the IP Binding Configuration page for models GS324T and GS324TP.

6. From the ACL ID menu, select the existing IP ACL for which you want to add an IP ACL interface binding.
   The fixed selection from the Direction menu is Inbound, which means that IP ACL rules are applied to traffic entering the interface.

7. In the Sequence Number field, optionally specify a number to indicate the order of the access list relative to other access lists already assigned to the interface and direction.
   A low number indicates high precedence order. If a sequence number is already in use for the interface and direction, the specified access list replaces the currently attached
access list using that sequence number. If you do not specify the sequence number (meaning that the value is 0), a sequence number that is one number greater than the highest sequence number currently in use for the interface and direction is used. The range is from 1 to 4294967295.

8. To add the selected ACL to a port or LAG, in the Ports table or LAG table, click the port or LAG so that a check mark displays.

You can add the ACL to several ports and LAGs.

The Ports and LAG tables display the available interfaces for ACL bindings. All nonrouting physical interfaces, VLAN interfaces, and interfaces participating in LAGs are listed.

9. Click the **Apply** button.

Your settings are saved.

The following table describes the nonconfigurable information displayed on the page.

<table>
<thead>
<tr>
<th><strong>Table 63. IP Binding Status table</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Interface</td>
</tr>
<tr>
<td>Direction</td>
</tr>
<tr>
<td>ACL Type</td>
</tr>
<tr>
<td>ACL ID/Name</td>
</tr>
<tr>
<td>Sequence Number</td>
</tr>
</tbody>
</table>

View or Delete IP ACL Bindings in the IP ACL Binding Table

You can view or delete IP ACL bindings.

**To view or delete IP ACL bindings:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.
4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **Security > ACL > Advanced > Binding Table**.

![IP ACL Binding Table](image)

6. To delete an IP ACL-to-interface binding, do the following:
   a. Select the check box next to the interface.
   b. Click the **Delete** button.
      The binding is removed.

The following table describes the information displayed in the IP ACL Binding Table.

**Table 64. IP ACL Binding Table**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface.</td>
</tr>
<tr>
<td>Direction</td>
<td>The selected packet filtering direction for the ACL, which is always Inbound.</td>
</tr>
<tr>
<td>ACL Type</td>
<td>The type of ACL assigned to the selected interface and direction.</td>
</tr>
<tr>
<td>ACL ID/Name</td>
<td>The ACL number (for an IP ACL) or ACL name (for a named IP ACL) identifying the ACL assigned to the selected interface and direction.</td>
</tr>
<tr>
<td>Sequence Number</td>
<td>The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.</td>
</tr>
</tbody>
</table>
Monitor the System

This chapter contains the following sections:

- Monitor the Switch and the Ports
- Configure and View Logs
- Configure Port Mirroring
Monitor the Switch and the Ports

The following sections describe how you can view a variety of information about the amount and type of traffic that is transmitted from and received on the switch:

- View Switch Statistics on page 294
- View Port Statistics on page 297
- View and Manage Detailed Port Statistics on page 300
- View or Clear EAP and EAPoL Statistics on page 306
- Perform a Cable Test (Model GS348T) on page 308

View Switch Statistics

You can view detailed statistical information about the traffic that the switch handles.

**To view or clear the switch statistics:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Ports > Switch Statistics**.
6. Click the **Refresh** button to refresh the page with the latest information about the switch.

7. Click the **Clear** button to clear all the statistics counters, resetting all switch summary and detailed statistics to default values.

   The discarded packets count cannot be cleared.

The following table describes the switch statistics displayed on the page.

**Table 65. Switch statistics**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifIndex</td>
<td>The interface index 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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 that were chosen to be discarded, even though no errors were 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 that were chosen to be discarded, even though no errors were 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 were 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 VLANs allowed on this switch.</td>
</tr>
<tr>
<td>Most VLAN Entries Ever Used</td>
<td>The largest number of VLANs that were active on this switch since the last reboot.</td>
</tr>
<tr>
<td>Static VLAN Entries</td>
<td>The number of active VLAN entries on this switch that were created statically.</td>
</tr>
<tr>
<td>VLAN Deletes</td>
<td>The number of VLANs on this switch that were 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>
View Port Statistics

You can view a summary of per-port traffic statistics on the switch.

To view port statistics:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Monitoring > Ports > Port Statistics.

6. Select whether to display physical interfaces, link aggregation groups (LAGs), or both by clicking one of the following links above the table heading:
   • 1 (or the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   • LAG. Only link aggregation groups are displayed.
   • All. Both physical interfaces and link aggregation groups are displayed.

7. Select one or more interfaces by taking one of the following actions:
   • To view a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
   • To view multiple interfaces, select the check box associated with each interface.
The following table describes the per-port statistics displayed on the page.

**Table 66. Port statistics**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface or LAG.</td>
</tr>
<tr>
<td>Total Packets Received</td>
<td>The total number of packets received that were without errors.</td>
</tr>
<tr>
<td>Without Errors</td>
<td></td>
</tr>
<tr>
<td>Packets Received With Error</td>
<td>The number of inbound packets that contained errors preventing them from</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>broadcast address. This does not include multicast packets.</td>
</tr>
<tr>
<td>Packets Transmitted Without</td>
<td>The number of frames without errors that were transmitted by the port.</td>
</tr>
<tr>
<td>Errors</td>
<td></td>
</tr>
<tr>
<td>Transmit Packet Errors</td>
<td>The number of outbound packets that could not be transmitted because of</td>
</tr>
<tr>
<td></td>
<td>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>Link Down Events</td>
<td>The total number of link down events on a physical port.</td>
</tr>
<tr>
<td>Time Since Counters Last</td>
<td>The elapsed time in days, hours, minutes, and seconds since the statistics</td>
</tr>
<tr>
<td>Cleared</td>
<td>for the port were last cleared.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Reset Counters for All Interfaces on the Switch

**To reset the counters for all interfaces on the switch:**

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   - The login window opens.

4. Enter the switch’s password in the **Password** field.
   - The default password is **password**.
   - The System Information page displays.

5. Select **Monitoring > Ports > Port Statistics**.
   - The Port Statistics page displays.

6. Select the check box in the heading of the table.
7. Click the **Clear** button.
   All counters are reset to 0.

Reset Counters for One or More Specific Interfaces

**To reset the counters for one or more specific interfaces:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is **password**.
   The System Information page displays.

5. Select **Monitoring > Ports > Port Statistics**.
   The Port Statistics page displays.

6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.

7. Select one or more interfaces by taking one of the following actions:
   - To reset a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To reset multiple interfaces, select the check box associated with each interface.

8. Click the **Clear** button.
   The counters for the interface are reset to 0.
View and Manage Detailed Port Statistics

You can view a variety of per-port traffic statistics.

To view and manage detailed port statistics:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Monitoring > Ports > Port Detailed Statistics.

The previous figure does not show all fields on the Port Detailed Statistics page.
6. From the Interface menu, select the interface for which you want to view the statistics.
7. From the MST ID menu, select the MST ID associated with the interface (if available).
8. To refresh the page with the latest information about the switch, click the Refresh button.
9. To clear all the counters, click the Clear button. This resets all statistics for the port to the default values.

The following table describes the detailed port information that displays for a particular port.

**Table 67. Detailed port statistics**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifIndex</td>
<td>The interface or LAG.</td>
</tr>
<tr>
<td>Port Type</td>
<td>For normal ports this field displays Normal. Otherwise, the options are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Mirrored. The port is a participating in port mirroring as a mirrored port.</td>
</tr>
<tr>
<td></td>
<td>• Probe. The port is a participating in port mirroring as the probe port.</td>
</tr>
<tr>
<td></td>
<td>• Port Channel. The port is a member of a LAG.</td>
</tr>
<tr>
<td>Port Channel ID</td>
<td>If the port is a member of a port channel (LAG), 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 is one of the following values: Root, Designated, Alternate, Backup, Master, or Disabled.</td>
</tr>
<tr>
<td>STP Mode</td>
<td>The Spanning Tree Protocol administrative mode that is associated with the port or port channel. The options are as follows:</td>
</tr>
<tr>
<td></td>
<td>• Enable. Spanning tree is enabled for the port.</td>
</tr>
<tr>
<td></td>
<td>• Disable. Spanning tree is disabled for the port.</td>
</tr>
<tr>
<td>STP State</td>
<td>The port's current Spanning Tree state. This state controls what action a port takes on receipt of a frame. If the bridge detects a malfunctioning port, it places that port into the broken state. The 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>The port control administration state. The port must be enabled for it to be allowed into the network. The default is Enabled.</td>
</tr>
<tr>
<td>Flow Control Mode</td>
<td>Indicates whether flow control is enabled or disabled for the port. This field does not apply to LAGs.</td>
</tr>
<tr>
<td>LACP Mode</td>
<td>Indicates the Link Aggregation Control Protocol administrative state. The mode must be enabled for the port to participate in link aggregation.</td>
</tr>
<tr>
<td>Physical Mode</td>
<td>Indicates the port speed and duplex mode. In autonegotiation mode the duplex mode and speed are set from the autonegotiation process.</td>
</tr>
<tr>
<td>Physical Status</td>
<td>Indicates the port speed and duplex mode for physical interfaces.</td>
</tr>
</tbody>
</table>
### Table 67. Detailed port statistics (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Status</td>
<td>Indicates whether the link is up or down.</td>
</tr>
<tr>
<td>Link Trap</td>
<td>Indicates whether or not the port sends a trap when 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 1519-2047 Octets</td>
<td>The total number of packets (including bad packets) received or transmitted that were between 1519 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets RX and TX 2048-4095 Octets</td>
<td>The total number of packets (including bad packets) received or transmitted that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets RX and TX 4096-9216 Octets</td>
<td>The total number of packets (including bad packets) received or transmitted that were between 4096 and 9216 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 you need greater precision, the etherStatsPkts and etherStatsOctets objects must 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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------</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>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; 1518 Octets</td>
<td>The total number of packets received that were longer than 1518 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>Receive Packets Discarded</td>
<td>The number of inbound packets that were discarded even though no errors were detected 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>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 included either a bad frame check sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (alignment error). This definition of jabber is different from 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 with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but included a bad frame check sequence (FCS) with a nonintegral number of octets.</td>
</tr>
</tbody>
</table>
Table 67. Detailed port statistics (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx FCS Errors</td>
<td>The total number of packets received with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but included 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 because the port was overloaded with incoming packets, and could not keep up with the inflow.</td>
</tr>
<tr>
<td>Total Received Packets Not</td>
<td>The number of valid frames received that were discarded (that is, filtered) by the forwarding process.</td>
</tr>
<tr>
<td>Forwarded</td>
<td></td>
</tr>
<tr>
<td>802.3x Pause Frames Received</td>
<td>The number of MAC control frames received on the 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 the port because of an unacceptable frame type.</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 you need greater precision, the etherStatsPkts and etherStatsOctets objects must 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) received 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) received 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) received 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) received 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) received 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) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Packets Transmitted &gt; 1518 Octets</td>
<td>The total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. This counter supports a maximum increment rate of 815 counts per sec at 10 Mb/s.</td>
</tr>
<tr>
<td>Maximum Frame Size</td>
<td>The maximum Ethernet frame size the interface supports or is configured to use, including Ethernet header, CRC, and payload. The possible range is 1518 to 9216. The default maximum frame size is 1518.</td>
</tr>
</tbody>
</table>
Table 67. Detailed port statistics (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Packets Transmitted</td>
<td>The number of frames that were transmitted by the port.</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 were detected to prevent them from 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>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 sent with a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but included a bad frame check sequence (FCS) with an integral number of octets.</td>
</tr>
<tr>
<td>Total Transmit Packets Discarded</td>
<td>The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.</td>
</tr>
<tr>
<td>Single Collision Frames</td>
<td>The number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.</td>
</tr>
<tr>
<td>Multiple Collision Frames</td>
<td>The number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.</td>
</tr>
<tr>
<td>Excessive Collision Frames</td>
<td>The number of frames for which transmission on a particular interface fails due to excessive collisions.</td>
</tr>
<tr>
<td>Dropped Transmit Frames</td>
<td>The number of transmit frames discarded at the selected port.</td>
</tr>
<tr>
<td>STP BPDUs Received</td>
<td>The number of STP BPDUs received at the selected port.</td>
</tr>
<tr>
<td>STP BPDUs Transmitted</td>
<td>The number of STP BPDUs transmitted from the selected port.</td>
</tr>
<tr>
<td>RSTP BPDUs Received</td>
<td>The number of RSTP BPDUs received at the selected port.</td>
</tr>
<tr>
<td>RSTP BPDUs Transmitted</td>
<td>The number of RSTP BPDUs transmitted from the selected port.</td>
</tr>
<tr>
<td>MSTP BPDUs Received</td>
<td>The number of MSTP BPDUs received at the selected port.</td>
</tr>
<tr>
<td>MSTP BPDUs Transmitted</td>
<td>The number of MSTP BPDUs transmitted from the selected port.</td>
</tr>
<tr>
<td>802.3x Pause Frames Transmitted</td>
<td>The number of MAC control frames transmitted on the 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>EAPOL Frames Received</td>
<td>The number of valid EAPoL frames of any type that were received by this authenticator.</td>
</tr>
</tbody>
</table>
You can view information about Extensible Authentication Protocol (EAP) and EAP over LAN (EAPoL) packets that are received on physical ports.

To view or clear EAP and EAPoL statistics:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the Password field.

   The default password is password.

   The System Information page displays.

5. Select Monitoring > Ports > EAP Statistics.

The previous figure does not show all fields on the EAP Statistics page.

6. To refresh the page with the latest information about the switch, click the Refresh button.

7. To clear the counters, which resets the EAP and EAPoL statistics to default values, take one of the following actions:

   - To clear the counters for a specific port, select the check box associated with the port, and click the Clear button.
• To clear the counters for multiple ports, select the check boxes associated with the ports, and click the **Clear** button.

• To clear all counters for all ports, select the check box in the row heading, and click the **Clear** button.

The following table describes the EAP statistics displayed on the page.

**Table 68. EAP statistics**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port number.</td>
</tr>
<tr>
<td>EAPOL Frames Received</td>
<td>The number of valid EAPoL frames of any type that were received by this authenticator.</td>
</tr>
<tr>
<td>EAPOL Frames Transmitted</td>
<td>The number of EAPoL frames of any type that were transmitted by this authenticator.</td>
</tr>
<tr>
<td>EAPOL Start Frames Received</td>
<td>The number of EAPoL start frames that were received by this authenticator.</td>
</tr>
<tr>
<td>EAPOL Logoff Frames Received</td>
<td>The number of EAPoL logoff frames that were received by this authenticator.</td>
</tr>
<tr>
<td>EAPOL Last Frame Version</td>
<td>The protocol version number carried in the most recently received EAPoL frame.</td>
</tr>
<tr>
<td>EAPOL Last Frame Source</td>
<td>The source MAC address carried in the most recently received EAPoL frame.</td>
</tr>
<tr>
<td>EAPOL Invalid Frames Received</td>
<td>The number of EAPoL frames that were received by this authenticator in which the frame type is not recognized.</td>
</tr>
<tr>
<td>EAPOL Length Error Frames Received</td>
<td>The number of EAPoL frames that were received by this authenticator in which the frame type is not recognized.</td>
</tr>
<tr>
<td>EAP Response/ID Frames Received</td>
<td>The number of EAP response/identity frames that were received by this authenticator.</td>
</tr>
<tr>
<td>EAP Response Frames Received</td>
<td>The number of valid EAP response frames (other than resp/ID frames) that were received by this authenticator.</td>
</tr>
<tr>
<td>EAP Request/ID Frames Transmitted</td>
<td>The number of EAP request/identity frames that were transmitted by this authenticator.</td>
</tr>
<tr>
<td>EAP Request Frames Transmitted</td>
<td>The number of EAP request frames (other than request/identity frames) that were transmitted by this authenticator.</td>
</tr>
</tbody>
</table>
Perform a Cable Test (Model GS348T)

On model GS348T, you can test and view information about the cables that are connected to switch ports.

**To perform a cable test:**

1. Connect your computer to the same network as the switch.  
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.  
   If you do not know the IP address of the switch, see *Discover or Change the Switch IP Address* on page 12.  
   The login window opens.
4. Enter the switch's password in the **Password** field.  
   The default password is **password**.  
   The System Information page displays.
5. Select **Monitoring > Ports > Cable Test**.

![Cable Test](image)

6. Select one or more interfaces by taking one of the following actions:
   - To test a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To test multiple interfaces, select the check box associated with each interface.
   - To test all interfaces, select the check box in the heading row.
7. Select the check boxes that are associated with the physical ports for which you want to test the cables.
8. Click the **Apply** button.

A cable test is performed on all selected ports. The cable test might take up to two seconds to complete. If the port forms an active link with a device, the cable status is always Normal. The test returns a cable length estimate if this feature is supported by the PHY for the current link speed. Note that if the link is down and a cable is attached to a
10/100 Ethernet adapter then the cable status might be Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded.

The following table describes the nonconfigurable information displayed on the page.

**Table 69. Cable Test information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable Status</td>
<td>Indicates the cable status:</td>
</tr>
<tr>
<td></td>
<td>• Normal. The cable is working correctly.</td>
</tr>
<tr>
<td></td>
<td>• Open. The cable is disconnected or a faulty connector exists.</td>
</tr>
<tr>
<td></td>
<td>• Short. An electrical short exists in the cable.</td>
</tr>
<tr>
<td></td>
<td>• Cable Test Failed. The cable status could not be determined. The cable might in fact be working.</td>
</tr>
<tr>
<td></td>
<td>• Untested. The cable is not yet tested.</td>
</tr>
<tr>
<td></td>
<td>• Invalid cable type. The cable type is unsupported.</td>
</tr>
<tr>
<td></td>
<td>• No cable. The cable is not present.</td>
</tr>
<tr>
<td>Cable Length</td>
<td>The estimated length of the cable in meters. The length is displayed as a range between the shortest estimated length and the longest estimated length. Unknown is displayed if the cable length could not be determined. The cable length is displayed only if the cable status is Normal.</td>
</tr>
<tr>
<td>Failure Location</td>
<td>The estimated distance in meters from the end of the cable to the failure location. The failure location is displayed only if the cable status is Open or Short.</td>
</tr>
</tbody>
</table>

### Configure and View Logs

The switch generates 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.

### Manage the Memory Logs

The memory log stores messages in memory based upon the settings for message component and severity. You can set the administrative status and behavior of logs in the system buffer. These log messages are cleared when the switch reboots.

**To configure the memory log settings and view or clear the memory log:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch. If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

The login window opens.

4. Enter the switch’s password in the Password field.

The default password is password.

The System Information page displays.

5. Select Monitoring > Logs > Memory Log.

The Memory Log page displays.

6. Select one of the following Admin Status radio buttons:
   - Enable. Enable system logging. This is the default setting.
   - Disable. Prevent the system from logging messages.

7. 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.

8. From the Severity Filter menu, select one of the following severity levels:
   - Emergency (0). System is unusable.
   - Alert (1). Action must be taken immediately.
   - Critical (2). Critical conditions.
   - Error (3). Error conditions.
   - Warning (4). Warning conditions.
   - Notice (5). Normal but significant conditions.
   - Informational (6). Informational messages.
   - Debug (7). Debug-level messages.

   **Note:** A log records messages equal to or above a configured severity threshold.

9. Click the Apply button.

   Your settings are saved.

   The Memory Log table displays on the Memory Log page.

   The Total number of Messages field displays the number of messages the system logged in memory. Only the 200 most recent entries are displayed on the page.

   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 through syslog support 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 1, which means it is a user-level message. Therefore, to determine the severity level of the message, subtract 8 from the number in the angle brackets. The sample log message shows a severity level of 6 (informational). For more information about the severity of a log message, see Manage the Server Log on page 313.

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 on to the HTTP management interface from a host with an IP address of 10.27.64.122.

10. To refresh the page with the latest information about the switch, click the Refresh button.

11. To clear the messages from the buffered log in the memory, click the Clear button.

**Manage the Flash Log**

The flash log is a persistent log, that is, a log that is stored in persistent storage. Persistent storage survives across platform reboots. The first log type is the system startup log. The system startup log stores the first 32 messages received after system reboot. The second log type is the system operation log. The system operation log stores messages received during system operation.

**To configure the flash log settings:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch's password in the Password field.
The default password is `password`.
The System Information page displays.

5. Select **Monitoring > Logs > FLASH Log**.

   The FLASH Log Configuration page displays.

6. Select one of the following Admin Status radio buttons:
   - **Enable**. A log that is enabled logs messages.
   - **Disable**. A log that is disabled does not log messages.

7. From the **Severity Filter** menu, select the logging level for messages that must be sent to the logging host.

   Log messages with the selected severity level and all log messages 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 warning level. If the device is down, or not functioning properly, an emergency log message is saved to the device.
   - **Alert** (1). The second-highest warning level. An alert log message is saved if a serious device malfunction occurs, such as all device features being down. Action must be taken immediately.
   - **Critical** (2). The third-highest warning level. A critical log message 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 occurred, such as a port being offline.
   - **Warning** (4). The lowest level of a device warning.
   - **Notice** (5). Normal but significant conditions. Provides the network administrators with device information.
   - **Informational** (6). Provides device information.
   - **Debug** (7). Provides detailed information about the device.

8. From the **Logs to be Displayed** menu, select one of the following options:
   - **Current Logs**. The log messages for the current switch session are displayed. This is the default setting.
   - **Previous Logs**. The previous log messages are displayed, that is, the log messages that are still in the flash memory from before the switch was rebooted.

9. Click the **Apply** button.

   Your settings are saved.

   The Total Number of Messages field shows is the total number of persistent log messages that are stored on the switch. The maximum number of persistent log messages displayed on the switch is 64.
Description: <15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 % Interface 12 transitioned to root state on message age timer expiry

The previous log message example indicates a user-level message (1) with severity 7 (debug) on a system that is not stacked and generated by component MSTP running in thread ID 2110 on Aug 24 05:34:05 by line 318 of file mspt_api.c. This is the 237th message logged. Messages logged to a collector or relay via syslog support an identical format as the previous message.

Manage the Server Log

You can let the switch send log messages to remote logging hosts.

You must enable the server log on the switch and specify one or more remote syslog hosts.

Enable the Server Log

To enable the server log:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Monitoring > Logs > Server Log.
   The Server Log Configuration page displays.

6. In the Server Log Configuration section, select one of the following Admin Status radio buttons:
   • Enable. Send log messages to all configured hosts (syslog collectors or relays) using the values configured for each host.
   • Disable. Stop logging to all syslog hosts. Disable means no messages are sent to any collector or relay.

7. In the Local UDP Port field, specify the port on the switch from which syslog messages must be sent. The Local UDP port values are 1 to 65535.

8. Click the Apply button.
Your settings are saved.

The Server Log Configuration section displays the following information:

- **Messages Received.** Shows the number of messages received by the log process. This includes messages that are dropped or ignored.
- **Messages Relayed.** 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.
- **Messages Ignored.** Shows the number of messages that were ignored.

**Add a Remote Syslog Host**

A remote syslog host is the same as a remote log server.

**To add a remote syslog host:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.
   
   The System Information page displays.

5. Select **Monitoring > Logs > Server Log**.
   
   The Server Log Configuration page displays.

6. In the Server Configuration section, specify the following settings:
   
   - **IP Address Type.** Specify the IP address type of the host, which can be **IPv4** or **DNS**.
   
   - **Host Address.** Specify the IP address or host name of the syslog host.
   
   - **Port.** Specify the port on the host to which syslog messages must be sent. The default port number is 514.
   
   - **Severity Filter.** Use the menu to select the severity of the logs that must be sent 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 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 a serious device malfunction occurs, 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 occurred, such as a port being 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.

7. Click the **Add** button.

   The remote syslog host is added.

   The Status field in the Server Configuration table shows whether the remote logging host is currently active.

**Modify the Settings for a Remote Syslog Host**

**To modify the settings for a remote syslog host:**

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address on page 12**.

   The login window opens.

4. Enter the switch’s password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Logs > Server Log**.

   The Server Log Configuration page displays.

6. In the table, select the check box that is associated with the host.

7. Change the information as needed.

8. Click the **Apply** button.

   Your settings are saved.
Delete the Settings for a Remote Syslog Host

**To delete the settings for a remote syslog host:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is `password`.
   The System Information page displays.

5. Select **Monitoring > Logs > Server Log**.
   The Server Log Configuration page displays.

6. In the table, select the check box that is associated with the host.

7. Click the **Delete** button.
   The host is removed.

---

View or Clear the Trap Logs and Counters

You can view information about the SNMP traps generated on the switch.
You can also display information about the traps that were sent.

**To view or clear the trap logs and the counters:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see [Discover or Change the Switch IP Address](#) on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is `password`. 
5. Select Monitoring > Logs > Trap Logs.

The System Information page displays.

6. To refresh the page with the latest information about the switch, click the Refresh button.

7. To clear the messages from the trap logs in the memory and clear the counters, click the Clear button.

The following table describes the Trap Log information that is displayed on the page.

Table 70. Trap Logs information

<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 occurred since the switch last rebooted.</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 overwrite the oldest entries.</td>
</tr>
<tr>
<td>Number of Traps since log last viewed</td>
<td>The number of traps that occurred since the traps were last displayed. Displaying the traps by any method (terminal interface display, web display, upload file from switch, and so on) causes this counter to be cleared to 0.</td>
</tr>
<tr>
<td>Log</td>
<td>The sequence number of this trap.</td>
</tr>
<tr>
<td>System Up Time</td>
<td>The time when 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>

View or Clear the Event Log

The event log contains error messages. The log can hold 2,000 entries and is erased when the switch attempts to add an entry after the log is full. The event log is preserved across system resets.
To view or clear the event log:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Monitoring > Logs > Event Logs.

6. To refresh the page with the latest information about the switch, click the Refresh button.

7. To clear the messages from the event logs in the memory, click the Clear button.

The following table describes the event log information that is displayed on the page.

Table 71. Event Logs information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry</td>
<td>The sequence number of the event.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of the event.</td>
</tr>
<tr>
<td>File Name</td>
<td>The file in which the event originated.</td>
</tr>
<tr>
<td>Line</td>
<td>The line number of the event.</td>
</tr>
<tr>
<td>Task Id</td>
<td>The task ID of the event.</td>
</tr>
<tr>
<td>Code</td>
<td>The event code.</td>
</tr>
<tr>
<td>Time</td>
<td>The time this event occurred.</td>
</tr>
</tbody>
</table>
Configure Port Mirroring

Port mirroring lets you select the network traffic of specific switch ports for analysis by a network analyzer. You can select many switch ports as source ports but a single switch port only as the destination port. You can configure how traffic is mirrored on a source port by selecting packets that are received, transmitted, or both.

A 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.

To globally enable port mirroring, specify the destination port, and specify one or more source ports:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.
   
   The System Information page displays.

5. Select Monitoring > Mirroring > Port Mirroring.
6. Select an Admin Mode radio button:
   - True. Port mirroring is enabled.
   - False. Port mirroring is disabled. This is the default setting.

7. From the Destination Port menu, select the physical destination port to which port traffic must be copied.
   
   You can configure one destination port only. The port functions as a probe port and receives traffic from all configured source ports. If no port is configured, None is displayed. The default is None.

8. Click the Apply button.
   
   Your settings are saved.

   In the Source Interface Configuration section, perform the following steps.

9. Click the Apply button.
   
   Your settings are saved.

   In the Source Interface Configuration section, perform the following steps.

10. Select whether to display physical interfaces, LAGs, the CPU, or all by clicking one of the following links above the table heading:
   
   - 1 (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - LAG. Only LAGs are displayed.
   - CPU. Only the CPU is displayed.
   - All. The physical interfaces, LAGs, and CPU are displayed.

11. Select one or more interfaces by taking one of the following actions:
   
   - To select a single interface, select the check box associated with the port, or type the port number in the Go To Interface field and click the Go button.
• To select multiple interfaces, select the check box associated with each interface. Traffic from the selected ports will be sent to the destination port.

12. From the Direction menu, specify the direction of the traffic that must be mirrored from the selected source ports:
   • None. No traffic direction is selected. This is the default setting.
   • Tx and Rx. Monitors both transmitted and received packets.
   • Rx. Monitors received (ingress) packets only.
   • Tx. Monitors transmitted (egress) packets only.

13. Click the Apply button.
   Your settings are saved.
   The Status field indicates the interface status.
7

Maintenance

This chapter contains the following sections:

- Reboot the Switch
- Reset the Switch to Its Factory Default Settings
- Export a File From the Switch
- Download a File to the Switch or Update the Firmware
- Manage Software Images
- Enable Remote Diagnostics
Reboot the Switch

You can reboot the switch from the local browser interface.

To reboot the switch:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.
4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.
5. Select Maintenance > Reset > Device Reboot.
   The Device Reboot page displays.
6. Select the check box.
7. Click the Apply button.
   A confirmation pop-up window opens.
8. Click the Yes button to confirm.
   The switch reboots.
Reset the Switch to Its Factory Default Settings

You can reset the system configuration to the factory default values. All changes that you made are lost. If the IP address changes, your web session might disconnect.

**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 and do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

**To reset the switch to the factory default settings:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Reset > Factory Default**.
   
   The Default Settings page displays.

6. Select the check box.

7. Click the **Apply** button.
   
   A confirmation pop-up window opens.

8. Click the **Yes** button to confirm.
   
   All configuration settings are reset to their factory default values. All changes that you made are lost, even if you saved the configuration.
S350 Series 24-Port (PoE+) and 48-Port Gigabit Ethernet Smart Managed Pro Switches

Export a File From the Switch

You can export configuration (ASCII) or log (ASCII log) files from the switch to a file server by using TFTP or to a computer by using HTTP.

The following sections describe how you can export a file from the switch:

- Use TFTP to Export a File From the Switch to a TFTP Server on page 325
- Use HTTP to Export a File from the Switch to a Computer on page 326

Use TFTP to Export a File From the Switch to a TFTP Server

You can upload (export) configuration (ASCII or log ASCII) files from the switch to a TFTP server on the network.

To export a file from the switch to a TFTP server:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Maintenance > Export > TFTP File Export.

6. From the File Type menu, select the type of file:
   - Text Configuration. A text-based configuration file enables you to edit a configured text file (startup-config) offline as needed. 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 or IP address), and download it to that device. This is the default setting.

- **Error Log.** The switch error log.
- **Trap Log.** The trap log with the switch trap records.
- **Buffered Log.** The switch buffered (in-memory) log.
- **Tech Support.** The tech support file is a text-base file that contains a variety of hardware, software, and configuration information that can assist in device and network troubleshooting.
- **Crash Logs.** The switch crash logs, if any are available.

7. From the **Server Address Type** menu, select the format for the **Server Address** field:
   - **IPv4.** Indicates that the TFTP server address is an IP address in dotted-decimal format. This is the default setting.
   - **DNS.** Indicates that the TFTP server address is a host name.

8. In the **Server Address** field, enter the IP address of the server in accordance with the format indicated by the server address type.
   The default is the IPv4 address 0.0.0.0.

9. In the **Transfer File Path** field, specify the path on the TFTP server where you want to save the file.
   You can 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.

10. In the **Transfer File Name** field, specify a destination file name for the file to be uploaded.
    You can enter up to 32 characters. The transfer fails if you do not specify a file name.

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

12. Click the **Apply** button.
    The file transfer begins.

    The page displays information about the file transfer progress. The page refreshes automatically when the file transfer completes.

Use HTTP to Export a File from the Switch to a Computer

You can upload (export) files of various types from the switch to a computer through an HTTP session by using your web browser.

**To export a file from the switch to a computer by using HTTP:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Maintenance > Export > HTTP File Export.
   The HTTP File Export page displays.

6. From the File Type menu, select the type of file:
   - **Text Configuration.** A text-based configuration file enables you to edit a configured text file (startup-config) offline as needed. 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 or IP address), and download it to that device.
   - **Tech Support.** The tech support file is a text-base file that contains a variety of hardware, software, and configuration information that can assist in device and network troubleshooting.
   - **Crash Logs.** The switch crash logs, if any are available.

7. Click the Apply button.
   The file transfer begins.
   The page displays information about the file transfer progress. The page refreshes automatically when the file transfer completes.

Download a File to the Switch or Update the Firmware

You can download system files from a remote system to the switch by using either TFTP or HTTP. In this context, downloading is also referred to as updating.

These procedures also include updating the switch firmware.

The following sections describe how you can download a file to the switch:

- Use TFTP to Download a File to the Switch or Update the Software Image on page 328
- Use HTTP to Download a File to the Switch or Update the Software Image on page 330
Use TFTP to Download a File to the Switch or Update the Software Image

You can download a software (firmware) image, configuration files, and SSL files from a TFTP server to the switch.

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 contains a path to the TFTP server.

You can also download files by using HTTP. See Use HTTP to Download a File to the Switch or Update the Software Image on page 330 for additional information.

To download a file to the switch from a TFTP server:

1. Connect your computer to the same network as the switch.
   - You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   - If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   - The login window opens.

4. Enter the switch's password in the Password field.
   - The default password is password.
   - The System Information page displays.

5. Select Maintenance > Update > TFTP Firmware/File Update.
6. From the **File Type** menu, select the type of file:
   - **Software.** 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 corrupted, the system automatically boots from the nonactive image. This is a safety feature for faults occurring during the boot upgrade process. This is the default setting.
   - **Text Configuration.** A text-based configuration file enables you to edit a configured text file (startup-config) offline as needed. 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 or IP address), and download it to that device.

7. If the selection from the **File Type** menu is **Software**, the **Image Name** menu is displayed and you must select the software image that must be downloaded to the switch:
   - **image1.** Select image1 to upload image1.
   - **image2.** Select image2 to upload image2.

   **Note:** We recommended that you do not overwrite the active image. If you do so, the switch displays a warning that you are trying to overwrite the active image.

8. From the **Server Address Type** menu, select the format for the **TFTP Server IP** field:
   - **IPv4.** Indicates that the TFTP server address is an IP address in dotted-decimal format. This is the default setting.
   - **DNS.** Indicates that the TFTP server address is a host name.

9. In the **TFTP Server IP** field, enter the IP address of the TFTP server indicated by the server address type.
   The default is the IPv4 address 0.0.0.0.

10. In the **Transfer File Path** field, specify the path on the TFTP server where the file is located.
    Enter up to 160 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.

11. In the **Remote File Name** field, specify the name of the file to download from the TFTP server.
    You can enter up to 32 characters. A file name with a space is not accepted.
12. Select the **Start File Transfer** check box to initiate the file upload.
13. Click the **Apply** button.

The file transfer begins.

The page displays information about the progress of the file transfer. The page refreshes automatically when the file transfer completes.

---

**Note:** After a software image file is downloaded, you might need to select the new software image file (see Change the Software Image That Loads When the Switch Starts or Reboots on page 333) and reboot the switch.

---

**Use HTTP to Download a File to the Switch or Update the Software Image**

You can download a software (firmware) image, configuration files, and SSL files from a computer to the switch by using an HTTP session over a web browser.

**To download a file to the switch using HTTP:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see **Discover or Change the Switch IP Address on page 12**.
   
   The login window opens.
4. Enter the switch’s password in the **Password** field.
   
   The default password is **password**.
   
   The System Information page displays.
5. Select **Maintenance > Update > HTTP Firmware/File Update**.
   
   ![Image of HTTP Firmware/File Update interface]

   **Note:** This process will send a file from your computer to the switch. When the file transfer starts, wait until the page refreshes before continuing.
6. From the **File Type** menu, select the type of file:
   - **Software.** 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, the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the nonactive image. This is a safety feature for faults occurring during the boot upgrade process. This the default setting.
   - **Text Configuration.** A text-based configuration file enables you to edit a configured text file (`startup-config`) offline as needed. 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.

7. If the selection from the **File Type** menu is **Software**, the **Image Name** menu is displayed and you must select the software image that must be downloaded to the switch:
   - **image1.** Select image1 to upload image1.
   - **image2.** Select image2 to upload image2.

   **Note:** We recommended that you do not overwrite the active image. If you do so, the switch displays a warning that you are trying to overwrite the active image.

8. Click the **Browse** button and locate and select the file that you want to download.
   The file name can contain up to 80 characters.

9. Click the **Apply** button.
   The file transfer begins.
   The page displays information about the progress of the file transfer. After a file transfer is started, wait until the page refreshes. When the page refreshes, the option to select a file option is no longer available, indicating that the file transfer is complete.

---

**Note:** After a software image file is downloaded, you might need to select the new software image file (see Change the Software Image That Loads When the Switch Starts or Reboots on page 333) and reboot the switch. After a text configuration file is downloaded, the switch applies the configuration automatically.

---
Manage Software Images

The switch maintains two versions of the switch software in permanent storage. One image is the active image, and the second image is the backup image. The active image is loaded when the switch starts or reboots. This feature reduces switch down time when you are updating the switch software.

Note: A switch that runs an older (legacy) software version might not load a configuration file that is created by a newer software version. In such a situation, the switch displays a warning.

The following sections describe how you can manage the software images:

- Copy a Software Image on page 332
- Configure Dual Image Settings on page 333

Copy a Software Image

You can copy a software image from one location (primary or backup) to another.

To copy a software image:

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Maintenance > File Management > Copy.
6. Select the Source Image image1 or image2 radio button to specify the image to be copied.

7. Select the Destination Image image1 or image2 radio button to specify the destination image.

8. Click the Apply button.
   Your settings are saved.

Configure Dual Image Settings

The Dual Image feature allows the switch to retain two images in permanent storage. You can select which image must load when the reboots, specify an image description, or delete an image. This feature reduces switch down time when you are upgrading or downgrading the software image.

Change the Software Image That Loads When the Switch Starts or Reboots

**To change the image that loads during the boot process:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the Password field.
   The default password is password.
   The System Information page displays.

5. Select Maintenance > File Management > Dual Image Configuration.

6. From the Image Name menu, select the image that is not the image displayed in the Current-active field but that is the image that you want the switch to run after it reboots.
   The Current-active field displays the name of the active image.
7. As an option, specify a name for the selected image by entering one in the **Image Description** field.
8. Select the **Activate Image** check box.
9. Click the **Apply** button.
   Your settings are saved.

**IMPORTANT:**

After activating an image, you must reboot the switch. Otherwise, the switch continues running the image shown in the Current-active field until the switch reboots.

Delete a Software Image

**To delete a software image:**

1. Connect your computer to the same network as the switch.
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   The login window opens.

4. Enter the switch’s password in the **Password** field.
   The default password is *password*.
   The System Information page displays.

5. Select **Maintenance > File Management > Dual Image Configuration**.
   The Dual Image Configuration page displays.

6. From the **Image Name** menu, select the image that is *not* the image displayed in the Current-active field.
   The Current-active field displays the name of the active image. You cannot delete the active image.

7. Select the **Delete** Image check box.

8. Click the **Apply** button.
   The image is removed.
View the Dual Image Status

You can view information about the active and backup images on the system.

**To view dual image status information:**

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > File Management > Dual Image > Dual Image Status**.

The following table describes the information available on the page.

**Table 72. Dual Image Status information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image1 Ver</td>
<td>The version of the image1 file.</td>
</tr>
<tr>
<td>Image2 Ver</td>
<td>The version of the image2 file.</td>
</tr>
<tr>
<td>Current-active</td>
<td>The currently active image on this switch.</td>
</tr>
<tr>
<td>Next-active</td>
<td>The image to be used after the switch reboots.</td>
</tr>
<tr>
<td>Image1 Description</td>
<td>The description associated with the image1 file.</td>
</tr>
<tr>
<td>Image2 Description</td>
<td>The description associated with the image2 file.</td>
</tr>
</tbody>
</table>
Enable Remote Diagnostics

You can enable or disable the option to access the switch remotely. When remote access is enabled, you or technical support can perform remote diagnostics services.

To enable remote diagnostics:

1. Connect your computer to the same network as the switch.
   
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.
   
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.
   
   The login window opens.

4. Enter the switch’s password in the Password field.
   
   The default password is password.
   
   The System Information page displays.

5. Select Maintenance > Troubleshooting > Remote Diagnostics.
   
   The Remote Diagnostics page displays.

6. Select the Enable radio button.

7. Click the Apply button.
   
   Your settings are saved.
A

Configuration Examples

This appendix contains the following sections:

- Virtual Local Area Networks (VLANs)
- Access Control Lists (ACLs)
- Differentiated Services (DiffServ)
- 802.1X Access Control
- Multiple Spanning Tree Protocol
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 computers, 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 set up the VLANs.

VLANs present a number of advantages:

- It is easy to do network segmentation. Users who 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 supports 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 on the Port PVID Configuration page. See Configure Port PVID Settings on page 129.
- 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 is not a member of the VLAN as specified by the VLAN ID tag, the packet is dropped.
VLAN Configuration Examples

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. On the Basic VLAN Configuration page (see Configure VLANs on page 122), create the following VLANs:
   - A VLAN with VLAN ID 10.
   - A VLAN with VLAN ID 20.

2. On the VLAN Membership page (see Configure VLAN Membership on page 125) 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. On the Port PVID Configuration page (see Configure Port PVID Settings on page 129), 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 can access 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 can access 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 can access 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 can access 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 sequential collections 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.

   The switch allow ACLs to be bound to physical ports and LAGs. The switch software supports MAC ACLs and IP ACLs.

MAC ACL Sample 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. On the MAC ACL page, create an ACL with the name Sales_ACL for the Sales department of your network (see Configure a Basic MAC ACL on page 266).

   By default, this ACL is bound on the inbound direction, which means that the switch examines traffic as it enters the port.
2. On the MAC Rules page, create a rule for the Sales_ACL with the following settings:
   • **Sequence Number**: 1
   • **Action**: Permit
   • **Assign Queue ID**: 0
   • **Match Every**: False
   • **CoS**: 0
   • **Destination MAC**: 01:02:1A:BC:DE:EF
   • **Destination MAC Mask**: 00:00:00:00:FF:FF
   • **EtherType**: User Value.
   • **Source MAC**: 02:02:1A:BC:DE:EF
   • **Source MAC Mask**: 00:00:00:00:FF:FF
   • **VLAN ID**: 2
   
   For more information about MAC ACL rules, see Configure MAC ACL Rules on page 266.

3. On the MAC Binding Configuration page, assign the Sales_ACL to the interface Gigabit ports 6, 7, and 8, and then click the Apply button. (See Configure MAC Bindings on page 272.)

   You can assign an optional sequence number to indicate the order of the access list relative to other access lists if any are already assigned to the interface and direction.

4. The MAC Binding Table displays the interface and MAC ACL binding information. (See View or Delete MAC ACL Bindings in the MAC Binding Table on page 274.)

   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 Sample 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. On the IP ACL page, create a new IP ACL with an IP ACL ID of 1. (See Configure a Basic or Extended IP ACL on page 275.)

2. On the IP Rules page, create a rule for IP ACL 1 with the following settings:
   • **Sequence Number**: 1
   • **Action**: Deny
3. Click the Add button.
4. On the IP Rules page, create a second rule for IP ACL 1 with the following settings:
   - **Sequence Number**: 2
   - **Action**: Permit
   - **Match Every**: True
5. Click the Add button.
6. On 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 Configure IP ACL Interface Bindings on page 289.)

   By default, this IP ACL is bound on the inbound direction, so it examines traffic as it enters the switch.
7. Click the Apply button.
8. Use the IP Binding Table page to view the interfaces and IP ACL binding information. (See View or Delete IP ACL Bindings in the IP ACL Binding Table on page 291)

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 an explicit *deny all* rule exists 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 delivers the data in a timely fashion, although there is no guarantee that it does. During times of congestion, packets might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. However, any degradation of service can negatively affect applications with strict timing requirements, such as voice or multimedia.

Quality of Service (QoS) can provide consistent, predictable data delivery by distinguishing between packets with 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 cannot meet the necessary timing requirements, this creates a deficiency in the network path and the performance of the entire packet flow is compromised.
Two basic types of QoS are supported:

- **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.

The switch supports DiffServ.

The DiffServ feature contains a number of conceptual QoS building blocks that you can use to construct a differentiated service network. Use these same blocks in different ways to build other types of QoS architectures.

You must configure three key QoS building blocks for DiffServ:
- Class
- Policy
- Service (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 and so on)
- Layer 4 source/destination ports
- Source/destination IP address

From a DiffServ point of view, two types of classes exist:
- 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 multifield (MF) classifiers:

- Layer 2; Layers 3, 4 (IP only)
- Protocol-based
- Address-based

You can combine these classifiers with logical AND 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, depending on the defined class type. Only classes of the same type can be nested; class nesting does not allow for the negation (exclude option) of the referenced class.

To configure DiffServ, you must define service levels, namely the forwarding classes/PHBs identified by a DSCP value, on the egress interface. You define these service levels 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, two types of policies exist:

- **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. Several distinct QoS actions are 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 coexist 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 3-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 (such as the DSCP or IP precedence value)
definition to convey some QoS characteristics to downstream switches that 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. Out-of-profile packets that are either in excess of the conformance specification or are nonconformant are dropped.

- **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. For more information, see Monitor the Switch and the Ports on page 294.

- **Assigning QoS Queue.** Directs a 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 a classified traffic stream to a specified egress port (physical or LAG). This can occur in addition to any marking or policing action. It can also be specified along with a QoS queue assignment.

### DiffServ Example Configuration

To create a DiffServ class and policy and attach them to a switch interface, follow these steps:

1. On the QoS Class Configuration page, create a new class with the following settings:
   - **Class Name.** Class1
   - **Class Type.** All

   For more information, see Configure a DiffServ Class on page 195.

2. Click the **Class1** hyperlink to view the DiffServ Class Configuration page 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, see Configure a DiffServ Class on page 195.

4. Click the **Apply** button.

5. On the Policy Configuration page, create a new policy with the following settings:
   - **Policy Selector.** Policy1
   - **Member Class.** Class1

   For more information, see Configure a DiffServ Policy on page 200.
6. Click the Add button.
   The policy is added.

7. Click the Policy1 hyperlink to view the Policy Class Configuration page 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
   • Confirm Action. Send
   • Violate Action. Drop

   For more information, see Configure a DiffServ Policy on page 200.

9. On the Service Configuration page, select the check box next to interfaces g7 and g8 to attach the policy to these interfaces, and then click the Apply button. (See Configure the DiffServ Service Interface on page 205.)

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 include 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. Packets that violate the committed rate and burst size are dropped.

802.1X Access Control

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 you might want 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 to provide a means of authenticating and authorizing devices attached to a LAN port with point-to-point connection characteristics. If the authentication and authorization process fails, access control prevents access to that port. In this context, a port is a single point of attachment to the LAN, such as a port of a MAC bridge and an association 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 supports a guest VLAN, which allows unauthenticated users 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 that the guest VLAN provides.

Another 802.1X feature is the ability to configure a port to enable or 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 by which it can offer services to other systems reachable through the LAN. Port-based network access control allows the operation of a switch’s ports to be controlled to ensure that access to its services is permitted only 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 when you 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:

<table>
<thead>
<tr>
<th>1. Authenticator</th>
<th>A port that enforces authentication before allowing access to services available through that port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Supplicant</td>
<td>A port that attempts to access services offered by the authenticator.</td>
</tr>
</tbody>
</table>

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 for you to complete an authentication exchange.

The switch supports 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 for the credentials to be checked, which determines 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 (1/0/5–1/0/8). These ports are available to visitors and must be authenticated before access is granted 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 was configured with a VLAN ID of 150 and VLAN name of Guest.

1. On the Port Authentication page, select ports 1/0/5, 1/0/6, 1/0/7, and 1/0/8.
2. From the Port Control menu, select Unauthorized.

The selection from the Port Control menu for all other ports on which authentication is not needed must be Authorized. When the selection from the Port Control menu is Authorized, the port is unconditionally put in a force-authorized state and does not require any authentication. When the selection from the Port Control menu is Auto, the authenticator PAE sets the controlled port mode.

3. In the Guest VLAN field for ports 1/0/5–1/0/8, 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 Configure a Port Security Interface on page 257 for information about the settings.

4. Click the Apply button.
5. On the 802.1X Configuration page, set the port based authentication state and guest VLAN mode to Enable, and then the Apply button. (See Configure the Global Port Security Mode on page 256.)

This example uses the default values for the port authentication settings, but you can configure several additional settings. 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. On the RADIUS Server Configuration page, 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 *Manage the RADIUS Settings on page 211*.

7. Click the **Add** button.

8. On the Authentication List page, configure the default list to use RADIUS as the first authentication method. (See *Configure Authentication Lists on page 223*.)

   This example enables 802.1X-based port security on the 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.

### Multiple Spanning Tree Protocol

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 in a way that is appropriate for STP and RSTP bridges.

An MSTP bridge can be configured to behave entirely as a RSTP bridge or an STP bridge. So, an IEEE 802.1s bridge inherently also supports IEEE 802.1w and IEEE 802.1D.

The MSTP algorithm and protocol provide simple and full connectivity for frames assigned to any 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 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 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 through 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. An MSTP bridge transmits 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 without any bridges attached that cannot receive and transmit MSTP BPDUs. The MST configuration identifier includes 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)

Because multiple instances of spanning tree exist, an MSTP state is 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 MSTI or CIST). For example, port A can be forwarding for instance 1 while discarding for instance 2. The port states changed since IEEE 802.1D specification.

To support multiple spanning trees, configure an MSTP bridge with an unambiguous assignment of VLAN IDs (VIDs) to spanning trees. For such a configuration, ensure the following:

1. The allocation of VIDs to FIDs is unambiguous.
2. Each FID that is 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 MSTI. The CIST is also an instance of spanning tree with an MSTID of 0.

VIDs might be not be allocated to an instance, 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 switch. The example network includes three different switches that serve different locations in the network. In this example, ports 1/0/1–1/0/5 are connected to host stations, so those links are not subject to network loops. Ports 1/0/6–1/0/8 are connected across switches 1, 2, and 3.

![MSTP Sample Configuration Diagram]

Perform the following procedures on each switch to configure MSTP:

1. On the VLAN Configuration page, create VLANs 300 and 500 (see Configure VLAN Settings on page 123).
2. On the VLAN Membership page, include ports 1/0/1–1/0/8 as tagged (T) or untagged (U) members of VLAN 300 and VLAN 500 (see Configure VLAN Settings on page 123).
3. On the STP Configuration page, enable the Spanning Tree State option (see Configure the STP Settings and View the STP Status on page 144).
   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. On the CST Configuration page, 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.

If you do not specify a root bridge and all switches are assigned the same bridge priority value, the switch with the lowest MAC address is elected as the root bridge (see Configure and View the CST Settings on page 146).

5. On the CST Port Configuration page, select ports 1/0/1–1/0/8 and select Enable from the STP Status menu (see Configure and View the CST Port Settings on page 148).

6. Click the Apply button.

7. Select ports 1/0/1–1/0/5 (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 the Apply button.
   You can use the CST Port Status page to view spanning tree information about each port.

9. On the MST Configuration page, create a MST instances with the following settings:
   • MST ID. 1
   • Priority. Use the default (32768)
   • VLAN ID. 300
   For more information, see View Rapid STP Information on page 152.

10. Click the Add button.

11. Create a second MST instance with the following settings
   • MST ID. 2
   • Priority. 49152
   • VLAN ID. 500

12. Click the Add button.

In this example, assume that Switch 1 became the root bridge for the MST instance 1, and Switch 2 became the root bridge for MST instance 2. Switch 3 supports hosts in the sales department (ports 1/0/1, 1/0/2, and 1/0/3) and in the HR department (ports 1/0/4 and 1/0/5). Switches 1 and 2 also include hosts in the sales and HR 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.
This appendix contains the following sections:

- Switch Default Settings
- General Feature Default Settings
- System Setup and Maintenance Settings
- Port Characteristics
- Traffic Control Settings
- Quality of Service Settings
- Security Settings
- System Management Settings
- Settings for Other Features
- Hardware Technical Specifications
## Switch Default Settings

The following table describes the switch default settings.

**Table 73. Switch default settings**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>192.168.0.239</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default gateway</td>
<td>192.168.0.254</td>
</tr>
<tr>
<td>Protocol</td>
<td>DHCP</td>
</tr>
<tr>
<td>Management VLAN ID</td>
<td>1</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>Eight characters</td>
</tr>
<tr>
<td>SNTP client</td>
<td>Enabled</td>
</tr>
<tr>
<td>Global logging</td>
<td>Enabled</td>
</tr>
<tr>
<td>RAM logging</td>
<td>Enabled (Severity level: info and above)</td>
</tr>
<tr>
<td>Persistent (FLASH) logging</td>
<td>Disabled</td>
</tr>
<tr>
<td>DNS</td>
<td>Enabled (No servers configured)</td>
</tr>
<tr>
<td>SNMP Traps</td>
<td>Enabled</td>
</tr>
<tr>
<td>Auto Save</td>
<td>Enabled</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Not configured</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Not configured</td>
</tr>
<tr>
<td>Denial of service protection</td>
<td>Disabled</td>
</tr>
<tr>
<td>Dot1x authentication (IEEE 802.1X)</td>
<td>Disabled</td>
</tr>
<tr>
<td>MAC-based port security</td>
<td>All ports are unlocked</td>
</tr>
<tr>
<td>Access control lists (ACL)</td>
<td>None configured</td>
</tr>
<tr>
<td>Protected ports</td>
<td>None</td>
</tr>
<tr>
<td>Advertised port speed</td>
<td>Maximum capacity</td>
</tr>
<tr>
<td>Ingress storm control (broadcast, multicast, and unknown unicast traffic)</td>
<td>Disabled</td>
</tr>
<tr>
<td>MAC table address aging</td>
<td>300 seconds (dynamic addresses)</td>
</tr>
<tr>
<td>Default VLAN ID</td>
<td>1</td>
</tr>
</tbody>
</table>
Table 73. Switch default settings (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default VLAN name</td>
<td>Default</td>
</tr>
<tr>
<td>Voice VLAN</td>
<td>Disabled</td>
</tr>
<tr>
<td>RADIUS-assigned VLANs</td>
<td>Disabled</td>
</tr>
<tr>
<td>Multiple Spanning Tree</td>
<td>Disabled</td>
</tr>
<tr>
<td>Link aggregation</td>
<td>No link aggregation groups (LAGs) configured</td>
</tr>
<tr>
<td>LACP system priority</td>
<td>32768</td>
</tr>
<tr>
<td>DiffServ</td>
<td>Enabled</td>
</tr>
<tr>
<td>IGMP snooping</td>
<td>Enabled</td>
</tr>
<tr>
<td>IGMP snooping querier</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

General Feature Default Settings

The following table describes the general feature default settings.

Table 74. General feature default settings

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual LAN (IEEE 802.1Q)</td>
<td></td>
</tr>
</tbody>
</table>
| Default VLANs                | • 1 (Default). All ports are members.  
|                              | • 4089 (Auto-Video). No ports are members.  |
| PVID                         | 1                                |
| Acceptable frame types       | Admit All                        |
| Ingress filtering            | Disabled                         |
| Port priority                | 0                                |
| Ports                        |                                  |
| Frame size                   | 1500                             |
| Flow control                 | Disabled                         |
| 802.1X                       |                                  |
| Port-based authentication state | Disabled                  |
| VLAN assignment mode         | Disabled                         |
| Dynamic VLAN creation mode   | Disabled                         |
Table 74. General feature default settings (continued)

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAPoL flood mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port control</td>
<td>Auto</td>
</tr>
<tr>
<td>Unauthenticated VLAN ID</td>
<td>0 (none)</td>
</tr>
<tr>
<td>Periodic reauthentication</td>
<td>Disabled</td>
</tr>
<tr>
<td>Reauthentication period</td>
<td>3600</td>
</tr>
<tr>
<td>Quiet period</td>
<td>60</td>
</tr>
<tr>
<td>Resending EAP request</td>
<td>30</td>
</tr>
<tr>
<td>Maximum number of EAP requests</td>
<td>2</td>
</tr>
<tr>
<td>Suppliant time-out period</td>
<td>30</td>
</tr>
<tr>
<td>Server time-out period</td>
<td>30</td>
</tr>
<tr>
<td><strong>STP/RSTP/MSTP, Global</strong></td>
<td></td>
</tr>
<tr>
<td>Spanning tree state</td>
<td>Enabled</td>
</tr>
<tr>
<td>STP operation mode</td>
<td>IEEE 802.1s RSTP</td>
</tr>
<tr>
<td>Configuration name</td>
<td>MAC address</td>
</tr>
<tr>
<td>Configuration revision level</td>
<td>0</td>
</tr>
<tr>
<td>Forwarding of BPDUs while STP is disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>CST bridge priority</td>
<td>32768</td>
</tr>
<tr>
<td>CST bridge maximum age</td>
<td>20</td>
</tr>
<tr>
<td>CST bridge hello time</td>
<td>2</td>
</tr>
<tr>
<td>CST Bridge forward delay</td>
<td>15</td>
</tr>
<tr>
<td>CST spanning tree maximum number of hops</td>
<td>20</td>
</tr>
<tr>
<td>MST default instance ID</td>
<td>0</td>
</tr>
<tr>
<td>MST instance 0 priority</td>
<td>32768</td>
</tr>
<tr>
<td>MST instance 0 VLAN IDs</td>
<td>1, 4089</td>
</tr>
<tr>
<td><strong>STP/RSTP/MSTP, Interface</strong></td>
<td></td>
</tr>
<tr>
<td>CST STP status</td>
<td>Enabled</td>
</tr>
<tr>
<td>CST auto edge</td>
<td>Enabled</td>
</tr>
<tr>
<td>CST fast link</td>
<td>Disabled</td>
</tr>
<tr>
<td>CST BDPU forwarding</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Table 74. General feature default settings (continued)

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>CST path cost</td>
<td>0</td>
</tr>
<tr>
<td>CST priority</td>
<td>128</td>
</tr>
<tr>
<td>CST external path cost</td>
<td>0</td>
</tr>
</tbody>
</table>

**Link Aggregation**

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lag name</td>
<td>ch&lt;n&gt; where n is 1 to 8</td>
</tr>
<tr>
<td>LAG capability (“Admin Mode”)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Hash mode</td>
<td>Option 3: source MAC, destination MAC, VLAN, EtherType, and incoming port associated with the packet</td>
</tr>
<tr>
<td>STP mode</td>
<td>Enabled</td>
</tr>
<tr>
<td>Link trap</td>
<td>Enabled</td>
</tr>
<tr>
<td>LAG type</td>
<td>Static</td>
</tr>
</tbody>
</table>

**Local Link Discovery Protocol (LLDP), Global**

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLV advertised interval</td>
<td>30</td>
</tr>
<tr>
<td>Hold multiplier</td>
<td>4</td>
</tr>
<tr>
<td>Reinitializing delay</td>
<td>2</td>
</tr>
<tr>
<td>Transmit delay</td>
<td>5</td>
</tr>
<tr>
<td>Fast start duration</td>
<td>3</td>
</tr>
</tbody>
</table>

**Local Link Discovery Protocol (LLDP), Interface**

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin status</td>
<td>Tx and Rx</td>
</tr>
<tr>
<td>Management IP address</td>
<td>Auto advertise</td>
</tr>
<tr>
<td>Notification</td>
<td>Disabled</td>
</tr>
<tr>
<td>Optional TLVs</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**DHCP Snooping, Global**

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP snooping mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>MAC address validation</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**DHCP Snooping, Interface**

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>Logging of invalid packets</td>
<td>Disabled</td>
</tr>
<tr>
<td>Rate Limit</td>
<td>None</td>
</tr>
</tbody>
</table>
Table 74. General feature default settings (continued)

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burst Interval</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Persistent Configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td>Local</td>
</tr>
<tr>
<td>Write delay</td>
<td>300</td>
</tr>
<tr>
<td><strong>Class of Service (CoS), Global</strong></td>
<td></td>
</tr>
<tr>
<td>Trust Mode</td>
<td>802.1p</td>
</tr>
<tr>
<td>802.1p to queue mapping (802.1p -&gt; queue)</td>
<td>0 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>1 -&gt; 0</td>
</tr>
<tr>
<td></td>
<td>2 -&gt; 0</td>
</tr>
<tr>
<td></td>
<td>3 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>4 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>5 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>6 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>7 -&gt; 3</td>
</tr>
<tr>
<td><strong>Note:</strong> By default, eight 802.1p priorities</td>
<td></td>
</tr>
<tr>
<td>are mapped to four CoS queues.</td>
<td></td>
</tr>
<tr>
<td>DSCP to queue mapping (DSCP -&gt; queue)</td>
<td>Class Selector:</td>
</tr>
<tr>
<td></td>
<td>(CS 0) 000000 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>(CS 1) 001000 -&gt; 0</td>
</tr>
<tr>
<td></td>
<td>(CS 2) 010000 -&gt; 0</td>
</tr>
<tr>
<td></td>
<td>(CS 3) 011000 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>(CS 4) 100000 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>(CS 5) 101000 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>(CS 6) 110000 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>(CS 7) 111000 -&gt; 3</td>
</tr>
<tr>
<td>Assured Forwarding:</td>
<td></td>
</tr>
<tr>
<td>(AF 11) 001010 -&gt; 0</td>
<td></td>
</tr>
<tr>
<td>(AF 12) 001100 -&gt; 0</td>
<td></td>
</tr>
<tr>
<td>(AF 13) 001110 -&gt; 0</td>
<td></td>
</tr>
<tr>
<td>(AF 21) 010010 -&gt; 0</td>
<td></td>
</tr>
<tr>
<td>(AF 22) 010100 -&gt; 0</td>
<td></td>
</tr>
<tr>
<td>(AF 23) 010110 -&gt; 0</td>
<td></td>
</tr>
<tr>
<td>(AF 31) 011010 -&gt; 1</td>
<td></td>
</tr>
<tr>
<td>(AF 32) 011100 -&gt; 1</td>
<td></td>
</tr>
<tr>
<td>(AF 33) 011110 -&gt; 1</td>
<td></td>
</tr>
<tr>
<td>(AF 41) 100010 -&gt; 1</td>
<td></td>
</tr>
<tr>
<td>(AF 42) 100100 -&gt; 1</td>
<td></td>
</tr>
<tr>
<td>(AF 43) 100110 -&gt; 1</td>
<td></td>
</tr>
</tbody>
</table>
### Table 74. General feature default settings (continued)

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP to queue mapping (DSCP -&gt; queue) (continued)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Expedited Forwarding:</td>
</tr>
<tr>
<td></td>
<td>(EF) 101110 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>Other:</td>
</tr>
<tr>
<td></td>
<td>(1) 000001 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>(2) 000010 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>(3) 000011 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>(4) 000100 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>(5) 000101 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>(6) 000110 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>(7) 000111 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>(9) 001001 -&gt; 0</td>
</tr>
<tr>
<td></td>
<td>(11) 001011 -&gt; 0</td>
</tr>
<tr>
<td></td>
<td>(13) 001101 -&gt; 0</td>
</tr>
<tr>
<td></td>
<td>(15) 001111 -&gt; 0</td>
</tr>
<tr>
<td></td>
<td>(17) 010001 -&gt; 0</td>
</tr>
<tr>
<td></td>
<td>(19) 010011 -&gt; 0</td>
</tr>
<tr>
<td></td>
<td>(21) 010101 -&gt; 0</td>
</tr>
<tr>
<td></td>
<td>(23) 010111 -&gt; 0</td>
</tr>
<tr>
<td></td>
<td>(25) 011001 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>(27) 011011 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>(29) 011101 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>(31) 011111 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>(33) 100001 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>(35) 100011 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>(37) 100101 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>(39) 100111 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>(41) 101001 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>(43) 101011 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>(45) 101101 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>(47) 101111 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>(49) 110001 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>(50) 110010 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>(51) 110011 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>(52) 110100 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>(53) 110101 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>(54) 110110 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>(55) 110111 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>(57) 111001 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>(58) 111010 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>(59) 111011 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>(60) 111100 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>(61) 111101 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>(62) 111110 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>(63) 111111 -&gt; 3</td>
</tr>
</tbody>
</table>
### Table 74. General feature default settings (continued)

<table>
<thead>
<tr>
<th>Feature Name/Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Class of Service (CoS), Interface</strong></td>
<td></td>
</tr>
<tr>
<td>Trust mode</td>
<td>802.1p</td>
</tr>
<tr>
<td>Interface shaping rate</td>
<td>0</td>
</tr>
<tr>
<td>802.1p to queue mapping (802.1p → queue)</td>
<td>0 -&gt; 1</td>
</tr>
<tr>
<td><strong>Note:</strong> By default, eight 802.1p priorities are mapped to four CoS queues.</td>
<td>1 -&gt; 0</td>
</tr>
<tr>
<td></td>
<td>2 -&gt; 0</td>
</tr>
<tr>
<td></td>
<td>3 -&gt; 1</td>
</tr>
<tr>
<td></td>
<td>4 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>5 -&gt; 2</td>
</tr>
<tr>
<td></td>
<td>6 -&gt; 3</td>
</tr>
<tr>
<td></td>
<td>7 -&gt; 3</td>
</tr>
<tr>
<td>Queue minimum bandwidth</td>
<td>0</td>
</tr>
<tr>
<td>Queue scheduler type</td>
<td>Weighted</td>
</tr>
<tr>
<td><strong>Auto-VoIP, Protocol-Based</strong></td>
<td></td>
</tr>
<tr>
<td>Auto VoIP mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>Prioritization type</td>
<td>Traffic class</td>
</tr>
<tr>
<td>Auto-VoIP traffic class</td>
<td>7</td>
</tr>
<tr>
<td><strong>Auto-VoIP, OUI-Based</strong></td>
<td></td>
</tr>
<tr>
<td>Auto VoIP mode</td>
<td>Disabled</td>
</tr>
<tr>
<td>Auto-VoIP VLAN</td>
<td>None</td>
</tr>
<tr>
<td>OUI-based priority</td>
<td>7</td>
</tr>
<tr>
<td><strong>L2 Loop Protection</strong></td>
<td></td>
</tr>
<tr>
<td>Global L2 loop protection (“Admin Mode”)</td>
<td>Disabled</td>
</tr>
<tr>
<td>TLV advertised interval</td>
<td>5</td>
</tr>
<tr>
<td>Maximum number of PDUs received</td>
<td>1</td>
</tr>
<tr>
<td>Recovery time</td>
<td>0</td>
</tr>
</tbody>
</table>
System Setup and Maintenance Settings

The following table describes the system setup and maintenance settings.

Table 75. System setup and maintenance settings

<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 address</td>
<td>1</td>
<td>DHCP enabled, 192.168.0.239</td>
</tr>
<tr>
<td>System name configuration</td>
<td>1</td>
<td>N/A</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 (local browser interface 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>

Port Characteristics

The following table describes the port characteristics.

Table 76. Port characteristics

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto negotiating speed and full/half duplex</td>
<td>All ports</td>
<td>Auto negotiation</td>
</tr>
<tr>
<td>Auto MDI/MDIX</td>
<td>For cross over cables on all ports</td>
<td>Enabled</td>
</tr>
<tr>
<td>802.3x flow control/back pressure</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port mirroring: TX, RX, Both</td>
<td>1</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port trunking (aggregation)</td>
<td>8</td>
<td>Preconfigured</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>Enabled</td>
</tr>
<tr>
<td>802.1s spanning tree</td>
<td>8 instances</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Traffic Control Settings

The following table describes the traffic control settings.

Table 77. Traffic control settings

<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>Default is 1500 bytes Maximum is 9216 bytes</td>
</tr>
</tbody>
</table>

Quality of Service Settings

The following table describes the Quality of Service settings.

Table 78. Quality of Service settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of queues</td>
<td>Models GS324T and GS324TP. 4 queues, Model GS348T. 8 queues</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>Egress rate limiting</td>
<td>All ports</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Security Settings

The following table describes the security settings.

**Table 79. Security settings**

<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 ACLs)</td>
<td>All MAC addresses allowed</td>
</tr>
<tr>
<td>IP ACL</td>
<td>100 (shared with MAC ACLs)</td>
<td>All IP addresses allowed</td>
</tr>
<tr>
<td>Password control access</td>
<td>1</td>
<td>Idle timeout = 5 mins.</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 Management Settings

The following table describes the system management settings.

**Table 80. System management settings**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-session web connections</td>
<td>4</td>
<td>Enabled</td>
</tr>
<tr>
<td>SNMPv1/v2</td>
<td>Maximum 5 community entries</td>
<td>Enabled (read, read/write communities)</td>
</tr>
<tr>
<td>SNMPv3</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>Enabled</td>
</tr>
<tr>
<td>Logging</td>
<td>5 logs: memory, flash, server, traps, and events</td>
<td>Memory, traps, and events logs are 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>
Settings for Other Features

The following table describes the settings for other features.

Table 81. Settings for other features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Sets Supported</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP snooping v1/v2/v3</td>
<td>All ports and VLANs</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>
<tr>
<td>Number of DHCP snooping bindings</td>
<td>8K</td>
<td>N/A</td>
</tr>
<tr>
<td>Number of DHCP static entries</td>
<td>1024</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Hardware Technical Specifications

The following table describes the hardware technical specifications.

Table 82. Hardware technical specifications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Model GS324T</th>
<th>Model GS324TP</th>
<th>Model GS348T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network interfaces</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Twenty-four (24)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/100/1000BASE-T RJ-45 copper ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Two (2) 1000BASE-X fiber SFP ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power consumption without PoE</td>
<td>From 6.5 W to 13.5W</td>
<td>From 11.1W to 16.3W</td>
<td>From 25.0 to 39.1W</td>
</tr>
<tr>
<td>Power consumption with PoE</td>
<td>N/A</td>
<td>From 11.1W to 229.9W</td>
<td>N/A</td>
</tr>
<tr>
<td>Switch PoE+ power budget</td>
<td>N/A</td>
<td>190W</td>
<td>N/A</td>
</tr>
<tr>
<td>Dimensions (W x D x H)</td>
<td>12.9 x 6.7 x 1.7 in.</td>
<td>13.0 x 8.1 x 1.7 in.</td>
<td>17.3 x 8.1 x 1.7 in.</td>
</tr>
<tr>
<td></td>
<td>(328 x 169 x 43 mm)</td>
<td>(330 x 206 x 43 mm)</td>
<td>(440 x 206 x 43 mm)</td>
</tr>
<tr>
<td>Weight</td>
<td>3.57 lb (1.62 kg)</td>
<td>5.93 lb (2.69 kg)</td>
<td>6.72 lb (3.05 kg)</td>
</tr>
</tbody>
</table>
Table 82. Hardware technical specifications (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Model GS324T</th>
<th>Model GS324TP</th>
<th>Model GS348T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fans</td>
<td>None</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Operating temperature</td>
<td>32º to 113ºF (0º to 45°C)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating humidity</td>
<td>95% maximum relative humidity, noncondensing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating altitude</td>
<td>10,000 ft (3,000 m) maximum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage temperature</td>
<td>–4º to 158ºF (–20º to 70ºC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage humidity</td>
<td>95% maximum relative humidity, noncondensing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage altitude</td>
<td>10,000 ft (3,000 m) maximum</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| For more information, see the data sheet, which you can download by visiting netgear.com/support/download/.