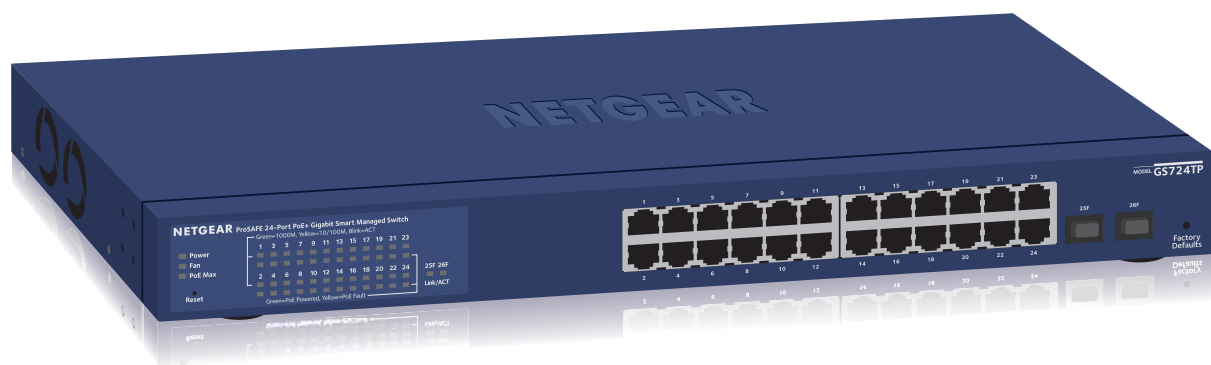




24-Port Gigabit Smart Managed Pro Switch with PoE+ and 2 SFP Ports Model GS724TPv2

User Manual



June 2017
202-11765-01

350 East Plumeria Drive
San Jose, CA 95134
USA



Support

Thank you for purchasing this NETGEAR product. You can visit 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.

Conformity

For the current EU Declaration of Conformity, visit http://kb.netgear.com/app/answers/detail/a_id/11621.

Compliance

For regulatory compliance information, visit <http://www.netgear.com/about/regulatory>.

See the regulatory compliance document before connecting the power supply.

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

Publication Part Number	Publish Date	Comments
202-11765-01	June 2017	First publication

Contents

Chapter 1 Get Started

Switch Management Interface Overview	9
Change the Default IP Address of the Switch	9
Discover a Switch in a Network With a DHCP Server	10
Discover a Switch in a Network Without a DHCP Server	11
Configure the Network Settings on Your Computer	12
Access the Web Browser–Based Management Interface	15
About the User Interfaces	15
Software Requirements to Use the Web Interface	15
Supported Web Browsers	16
Use a Web Browser to Access the Switch and Log In	16
Navigation Tabs, Configuration Menus, and Page Menu	17
Configuration and Status Options	18
Web Interface Buttons	18
User-Defined Fields	18
Web Browser–Based Management Interface Device View	19
Interface Naming Conventions	21
Configure Interface Settings	21
Context–Sensitive Help and Access to the Support WebSite	25
User Guide	26
Register Your Product	27

Chapter 2 Configure System Information

View and Configure the Switch Management Settings	29
View or Define System Information and View Software Information	29
Configure the Switch IP Settings	31
Configure the IPv6 Network Interface	33
View the IPv6 Network Neighbor	34
Configure the Time Settings	35
Configure Denial of Service Settings	50
Configure DNS Settings	52
Configure Green Ethernet Settings	56
Use the Device View	58
Configure PoE	58
Configure PoE Trap Settings and View PoE Information	59
Configure the PoE Port Settings	60
Configure SNMP	63
Configure the SNMPv1/v2 Community	63
Configure SNMPv1/v2 Trap Settings	65

Configure SNMPv1/v2 Trap Flags	68
View the Supported MIBs	69
Configure SNMP V3 Users.....	70
Configure LLDP	71
Configure LLDP Global Settings	71
Configure LLDP Port Settings.....	73
View LLDP-MED Network Policy Information	74
Configure LLDP-MED Port Settings	76
View Local LLDP Information	77
View LLDP Neighbors Information.....	79
Configure DHCP Snooping	82
Set Up PoE Timer Schedules	87
Create a PoE Timer Schedule	87
Specify the Settings for a PoE Timer Schedule	88
Delete a PoE Timer Schedule.....	90

Chapter 3 Configure Switching

Configure Port Settings	93
Configure Link Aggregation Groups.....	95
Configure LAG Settings	96
Configure LAG Membership	97
Set the LACP System Priority	98
Set the LACP Port Priority Settings.....	99
Configure VLANs.....	100
Configure VLAN Settings.....	101
Configure VLAN Membership	103
View VLAN Status	105
Configure Port PVID Settings	106
Configure a Voice VLAN	108
Configure Auto-VoIP	110
Configure Protocol-Based Port Settings.....	110
Configure Auto-VoIP OUI-Based Properties	111
Configure OUI-Based Port Settings.....	112
Manage the OUI Table	113
Display the Auto-VoIP Status	116
Configure Spanning Tree Protocol.....	117
Configure STP Settings	117
Configure CST Settings	119
Configure CST Port Settings.....	121
View CST Port Status	122
View Rapid STP Information	124
Manage MST Settings	125
Configure the MST Port Settings.....	127
View STP Statistics	130
Configure Multicast.....	131
View the MFDB Table.....	131
View the MFDB Statistics	132

IGMP Snooping Overview	133
Configure IGMP Snooping	134
Configure IGMP Snooping for Interfaces	135
View the IGMP Snooping Table	137
Configure IGMP Snooping for VLANs	138
Modify IGMP Snooping Settings for a VLAN	139
IGMP Snooping Querier Overview	140
Configure IGMP Snooping Querier	140
Configure IGMP Snooping Querier for VLANs	141
Display IGMP Snooping Querier for VLAN Status	142
Configure a Static Multicast Group	143
Remove a Static Multicast Group	144
Configure Multicast Group Membership	145
Configure the Multicast Forward All Option	147
View and Configure the MAC Address Table	148
Configure the MAC Address Table	148
Set the Dynamic Address Aging Interval	150
Configure a Static MAC Address	151

Chapter 4 Configure Quality of Service

Manage Class of Service	153
CoS Configuration Overview	153
Configure Global CoS Settings	153
Configure CoS Interface Settings for an Interface	155
Configure CoS Queue Settings for an Interface	156
802.1p to Queue Mapping	158
DSCP to Queue Mapping	159
Manage Differentiated Services	160
DiffServ Configuration Overview	161
Configure DiffServ Settings	161
Enable the DiffServ Mode and View the DiffServ Status	161
Configure a DiffServ Class	163
Configure a DiffServ Policy	168
Configure the DiffServ Service Interface	174
View DiffServ Service Statistics	176

Chapter 5 Manage Device Security

Configure the Management Security Settings	179
Change the Password	179
Configure RADIUS Servers	180
Configure TACACS+	189
Configure Authentication Lists	191
Configure Management Access	194
Configure HTTP Settings	194
Configure HTTPS Settings	195
Manage Certificates	197
Download Certificates	198

Configure Access Control	200
Configure Access Rule Settings	201
Configure Port Authentication	202
Configure Global 802.1X Settings	203
Manage Port Authentication	204
View the Port Summary	208
Configure Traffic Control	210
Manage MAC Filtering	210
MAC Filter Summary	212
Configure Storm Control	212
Configure Port Security	214
Configure Protected Ports	218
Configure Access Control Lists	219
Use the ACL Wizard to Create a Simple ACL	220
Configure a MAC ACL	225
Configure MAC ACL Rules	227
Configure MAC Bindings	231
View or Delete MAC ACL Bindings in the MAC Binding Table	233
Configure an IP ACL	234
Configure Rules for a Basic IP ACL	236
Configure Rules for an Extended IP ACL	240
Configure IP ACL Interface Bindings	244
View or Delete IP ACL Bindings in the IP ACL Binding Table	246

Chapter 6 Monitor the System

Monitor the Switch and the Ports	249
View Switch Statistics	249
View Port Statistics	252
View Detailed Port Statistics	254
View EAP Statistics	260
Perform a Cable Test	262
Configure and View Logs	263
Manage the Memory Logs	263
Message Log Format	265
Manage the Flash Log	266
Manage the Server Log	267
View the Trap Logs	270
Configure Port Mirroring	272

Chapter 7 Maintenance

Reboot the Switch	276
Reset the Switch to Its Factory Default Settings	276
Upload a File From the Switch	277
Upload a File to the TFTP Server	277
Upload a File Using HTTP	279
Download a File to the Switch	280

Download a File to the Switch Using TFTP	280
Download a File to the Switch Using HTTP	282
Manage Files	284
Configure Dual Image Settings	284
Delete an Image	285
Display the Dual Image Status	286
Perform Troubleshooting	287
Ping an IPv4 Address	287
Ping an IPv6 Address	288
Enable and Perform Remote Diagnostics	289

Appendix A Configuration Examples

Virtual Local Area Networks (VLANs)	292
VLAN Configuration Examples	293
Access Control Lists (ACLs)	294
MAC ACL Sample Configuration	294
Standard IP ACL Sample Configuration	295
Differentiated Services (DiffServ)	296
Class	297
DiffServ Traffic Classes	298
Creating Policies	298
DiffServ Example Configuration	299
802.1X	300
802.1X Example Configuration	302
MSTP	303
MSTP Example Configuration	305

Appendix B Specifications and Default Settings

Switch Default Settings	308
General Feature Default Settings	309
System Setup and Maintenance Settings	314
Port Characteristics	315
Traffic Control Settings	315
Quality of Service Settings	316
Security Settings	316
System Management Settings	317
Settings for Other Features	317

Get Started

1

This manual describes how you can configure and operate the NETGEAR 24-Port Gigabit Smart Managed Pro Switch with PoE+ and 2 SFP Ports, Model GS724TPv2 by using the web-based management interface. The manual describes the software configuration procedures and explains the options that are available within those procedures.

This chapter provides an overview of how you can start your switch and access the web-based management interface. The chapter contains the following sections:

- *Switch Management Interface Overview*
- *Change the Default IP Address of the Switch*
- *Discover a Switch in a Network With a DHCP Server*
- *Discover a Switch in a Network Without a DHCP Server*
- *Configure the Network Settings on Your Computer*
- *Access the Web Browser–Based Management Interface*
- *About the User Interfaces*
- *Use a Web Browser to Access the Switch and Log In*
- *Web Browser–Based Management Interface Device View*
- *Interface Naming Conventions*
- *Configure Interface Settings*
- *Context-Sensitive Help and Access to the Support WebSite*
- *Register Your Product*

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

Note: Firmware updates with new features and bug fixes are made available from time to time at downloadcenter.netgear.com. 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.

Switch Management Interface Overview

The switch provides administrative management options that let you configure, monitor, and control the network. Using the web browser–based management 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 the Smart Control Center (SCC) program, which runs on a Windows-based computer and is included on the resource CD. You can also download the SCC program from downloadcenter.netgear.com. If you do not use a Windows-based computer, 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 web browser–based management 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 downloadcenter.netgear.com.

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.

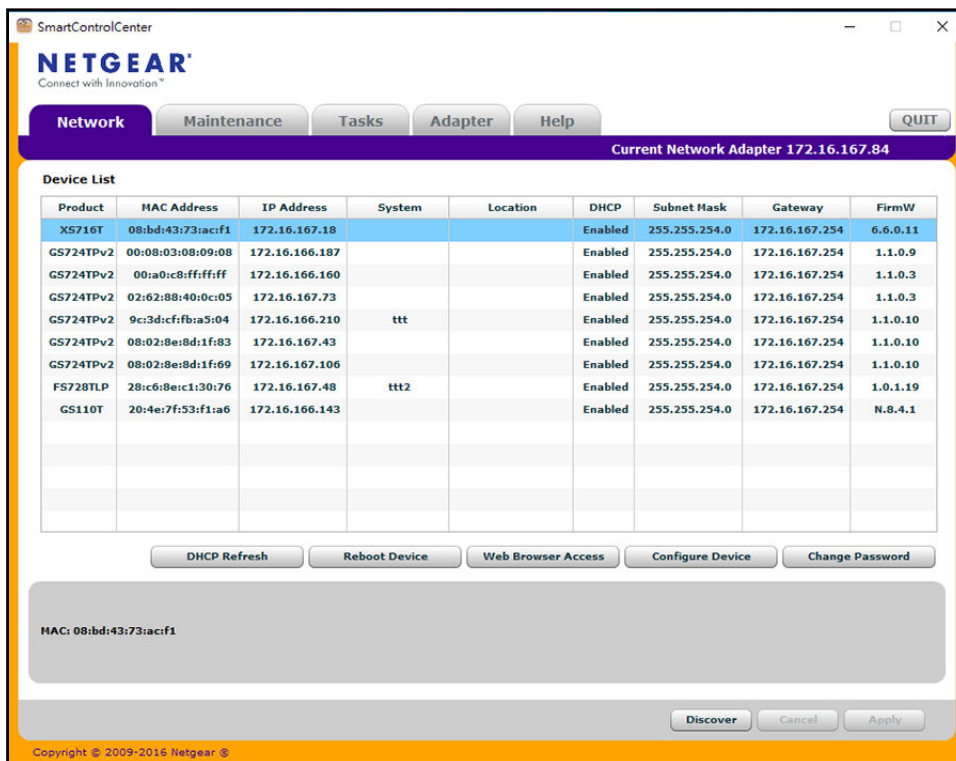
To change the default IP address of the switch, use one of the following methods:

- **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 a Switch in a Network With a DHCP Server](#) on page 10.
- **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 a Switch in a Network Without a DHCP Server](#) on page 11.
- **Static assignment by connecting from a local host.** If you do not want to use the Smart Control Center to assign a static address, you can connect to the switch from a host (administrative system) in the 192.168.0.0/24 network and change the settings by using the web browser–based management interface on the switch. For information about how to set the IP address on the administrative system so that it is in the same subnet as the default IP address of the switch, see [Configure the Network Settings on Your Computer](#) on page 12.

Discover a 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 to discover the IP address automatically assigned to the switch.

- **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 find your switch.



6. Make a note of the displayed IP address assigned by the DHCP server. You need this address later to access the switch directly from a web browser (without using the Smart Control Center).

GS724TPv2	00:08:03:08:09:08	172.16.166.187
GS724TPv2	00:a0:c8:ff:ff:ff	172.16.166.160

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 [Use a Web Browser to Access the Switch and Log In](#) on page 16.

Discover a Switch in a Network Without a DHCP Server

This section describes how to use the Smart Control Center to set up your switch in a network without a DHCP server. If your network 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.

➤ **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.

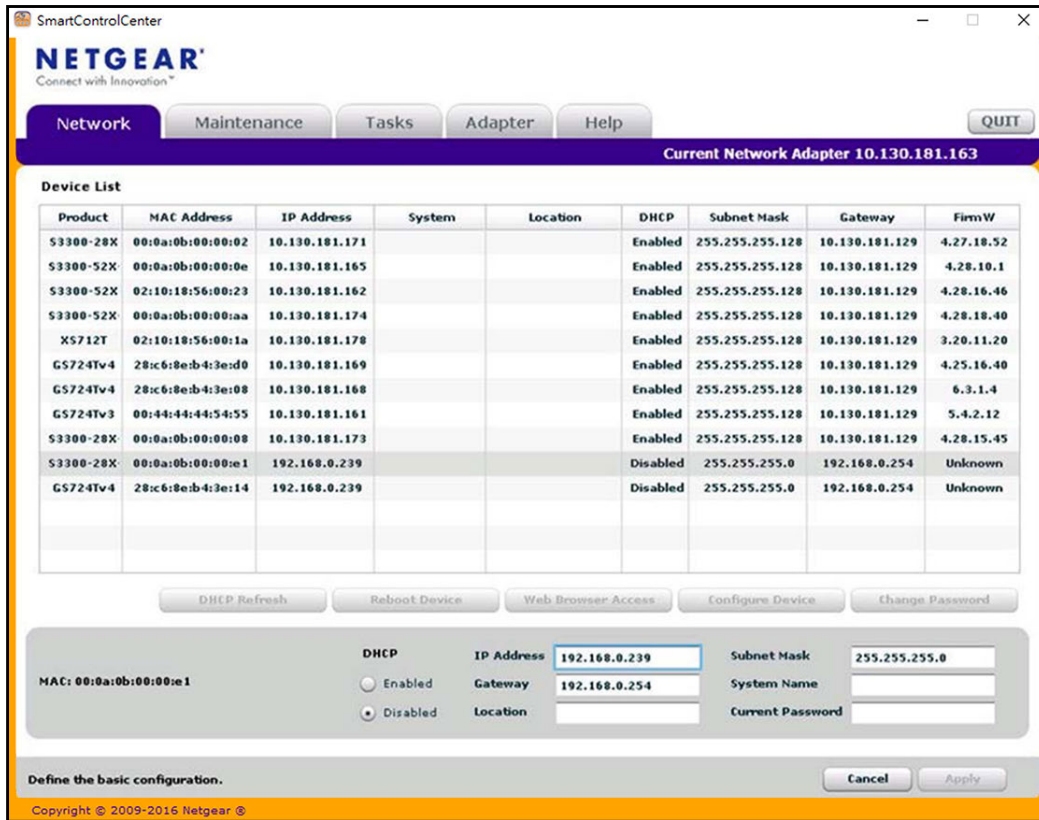
6. Select the switch, and then click the **Configure Device** button.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure the Network Settings on Your Computer

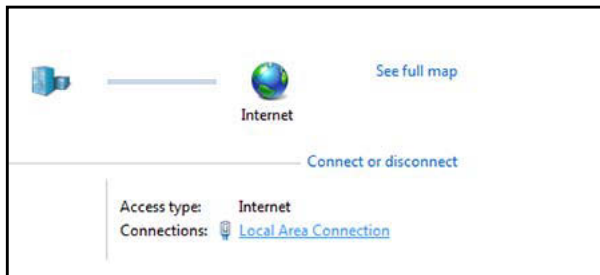
If you do not want to use the Smart Control Center to configure the network information on the switch, you can connect directly to the switch from an administrative system, such as a computer. The IP address of the computer must be in the same subnet as the default IP address on the switch. For most 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).

The method to change the IP address on a computer varies depending on the operating system version. You need Windows administrator privileges to change these settings. The

following procedures show how to change the static IP address on a computer running a Microsoft Windows 7.

➤ **To modify the network settings on your computer:**

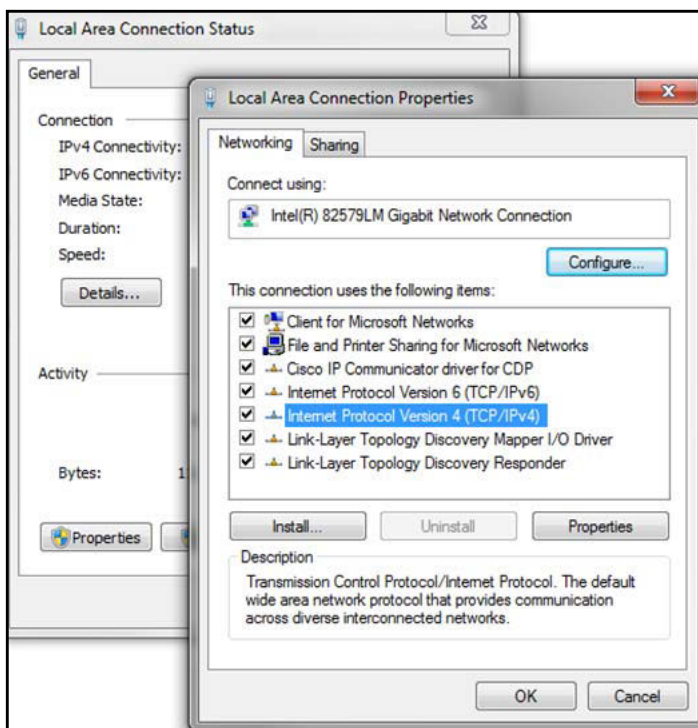
1. Open the Control Panel and click the **Network and Sharing Center** option.



2. Click the **Local Area Connection** link.

The Local Area Connection Status pop-window opens.

3. Click the **Properties** button.



4. Select **Internet Protocol Version 4 (TCP/IPv4)**.

5. Click the **Properties** button.

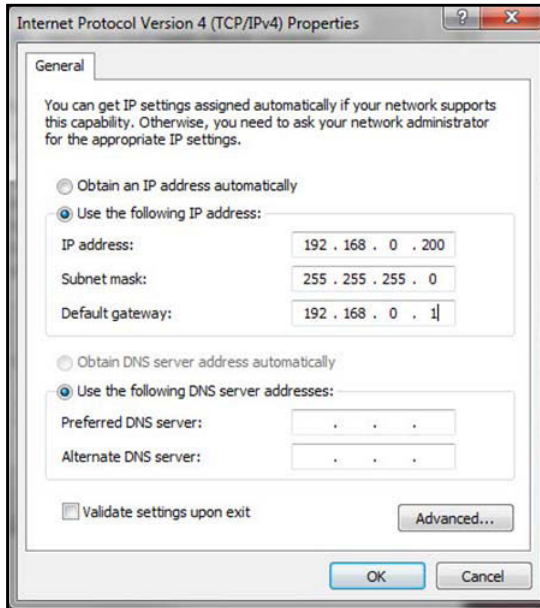
The Internet Protocol Version 4 (TCP/IPv4) Properties pop-up window opens.

6. Select the **Use the following IP address** radio button and change the IP address of the computer to an address in the 192.168.0.0 network, such as 192.168.0.200.

The IP address must be different from that of the switch but within the same subnet.

**WARNING:**

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



7. Click the **OK** button.
8. Close all other pop-up windows.

➤ **To configure a static address on the switch:**

1. Use a straight-through cable to connect the Ethernet port on the administrative system directly to any port on the switch.
2. Open a web browser on your computer and connect to the management interface.

For more information, see [Access the Web Browser–Based Management Interface](#) on page 15.

3. Change the network settings on the switch to match those of your network.

For more information, see [Configure the Switch IP Settings](#) on page 31.

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

Access the Web Browser–Based Management Interface

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

To access the switch web browser–based management interface, use one of the following methods:

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

Clicking the **Web Browser Access** button on the Smart Control Center or accessing the switch directly from your web browser displays the Login page.

Note: For more information about the Smart Control Center (SCC) program, see the SCC user manual that is included on the resource CD. You can also download the SCC program from downloadcenter.netgear.com.

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:

- Web browser–based management 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 web browser–based interface to manage and monitor the system.

Software Requirements to Use the Web Interface

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

- HTML version 4.0, or later
- HTTP version 1.1, or later

Supported Web Browsers

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

- Microsoft Internet Explorer (IE) versions 10–12
- Mozilla Firefox versions 18–52
- Chrome versions 28–58
- Opera Versions 26–44
- Safari on Windows OS 5.1.7
- Safari on MAC OS: 10.1

Use a Web Browser to Access the Switch and Log In

You can use a web browser to access the switch and log in. You must be able to ping the IP address of the switch management interface from your administrative system for web access to be available.

➤ To use browser–based access to log in to 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 [Change the Default IP Address of the Switch](#) on page 9.

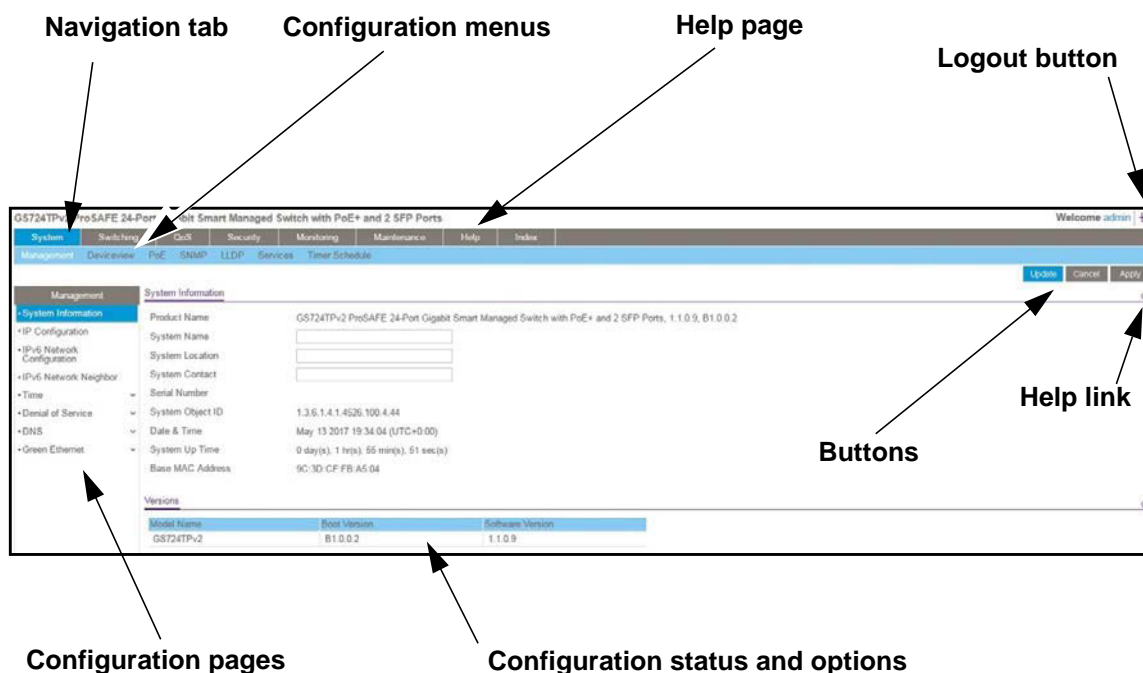
The login window opens.

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

The default password is **password**.

The Switch Information page displays.

The following figure shows the layout of the web interface.

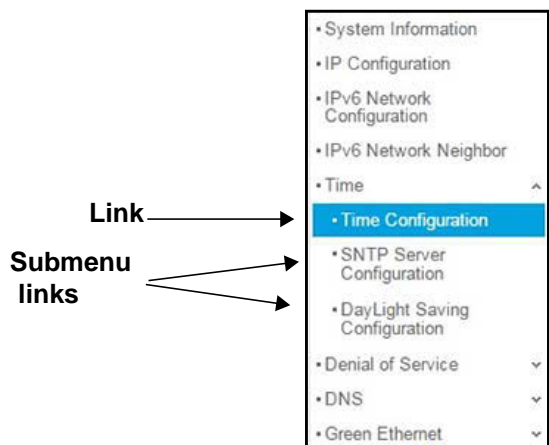


Navigation Tabs, Configuration Menus, and Page Menu

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

When you select a tab, the features for that tab appear as 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.

Web Interface Buttons

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

Table 1. Web interface command buttons

Button	Function
Add	Clicking the Add button adds the new item configured in the heading row of a table.
Apply	Clicking the Apply button sends the updated configuration to the switch. Configuration changes take effect immediately.
Cancel	Clicking the Cancel button cancels the configuration on the page and resets the data on the page to the previous values of the switch.
Delete	Clicking the Delete button removes the selected item.
Update	Clicking the Update button refreshes the page with the latest information from the device.
Logout	Clicking the Logout button ends the session.

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

Invalid Characters for user-defined fields	
\	<
/	>
*	
?	

Web Browser–Based Management Interface Device View

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 [Change the Default IP Address of the Switch](#) on page 9.

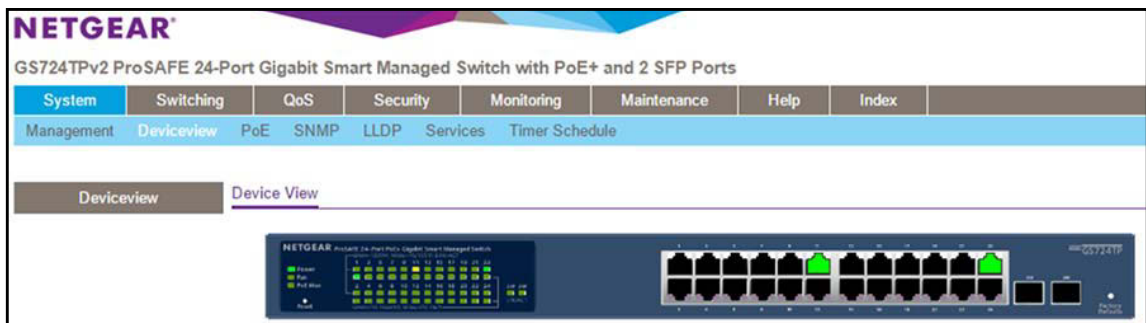
The login window opens.

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

The default password is **password**.

The Switch Information page displays.

5. Select **System > Device View**.



Depending upon the status of the port, the port color in Device View is either red, green, or black.

- Green indicates that the port is linking up.
- Red indicates that an error occurred on the port or that the port is administratively disabled.
- Black indicates that no link is present.

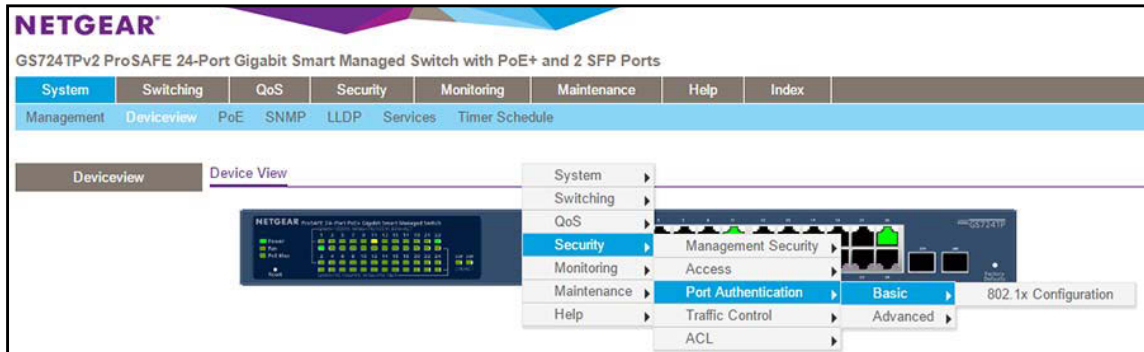
Each port also provides two LEDs in Device View to indicate the link status of the port.

- The green LED indicates that the port is linking at a speed of 1 Gbps.
- The yellow LED indicates that the port is linking at a speed of 100 Mbps or 10 Mbps.

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.



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

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

- **Solid green.** The power is supplied to the switch and operating normally.
- **Solid yellow.** The system is in the boot-up stage.
- **Off.** No power is supplied to the switch.

Fan LED

The Fan LED indicates the following status:

- **Solid yellow.** The fan is faulty.
- **Off.** The fan is operating normally.

PoE Max LED

The PoE Max LED indicates the following status:

- **Solid amber.** Less than 7W of PoE power is available.
- **Blinking amber.** At least once during the previous two minutes, less than 7W of PoE power was available.
- **Off.** Sufficient (more than 7W of) PoE power is 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 3. Naming conventions for interfaces

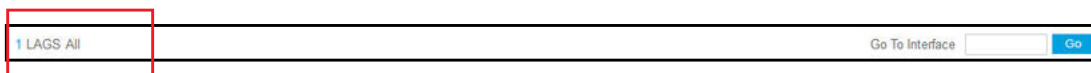
Interface	Description	Example
Physical	The physical ports are 1 Gigabit Ethernet interfaces and are numbered sequentially starting from 1.	g1, g2, g12
Link aggregation group (LAG)	LAG interfaces are logical interfaces that are used only for bridging functions.	l1, l2, l3
CPU management interface	This is the internal switch interface responsible for the switch base MAC address. This interface is not configurable and is always listed in the MAC Address Table.	c1

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:

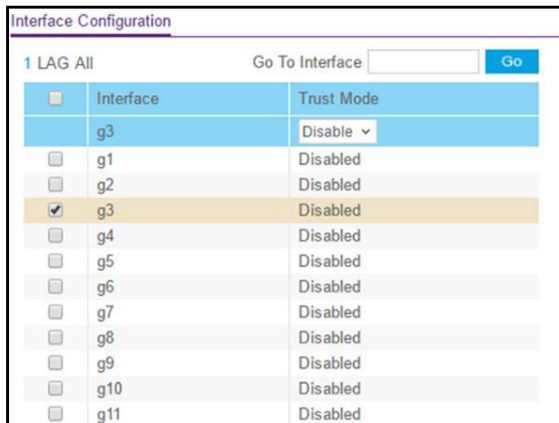
- To display all ports, click the **1** link.
- To display all LAGs, click the **LAG** link.
- To display all ports and LAGs, click the **All** link.

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 [Use a Web Browser to Access the Switch and Log In](#) on page 16.

➤ **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 g3.
For more information, see [Interface Naming Conventions](#) on page 21.
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.



Interface Configuration		
1 LAG All	Go To Interface	Go
<input type="checkbox"/>	Interface	Trust Mode
<input checked="" type="checkbox"/>	g3	Disable ▾
<input type="checkbox"/>	g1	Disabled
<input type="checkbox"/>	g2	Disabled
<input checked="" type="checkbox"/>	g3	Disabled
<input type="checkbox"/>	g4	Disabled
<input type="checkbox"/>	g5	Disabled
<input type="checkbox"/>	g6	Disabled
<input type="checkbox"/>	g7	Disabled
<input type="checkbox"/>	g8	Disabled
<input type="checkbox"/>	g9	Disabled
<input type="checkbox"/>	g10	Disabled
<input type="checkbox"/>	g11	Disabled

4. Configure the desired settings.
5. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

➤ **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 21.
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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

➤ **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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

➤ **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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

➤ **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.

The screenshot shows the 'Interface Configuration' page. At the top, there is a 'Go To Interface' search box and a 'Go' button. Below this is a table with columns for 'Interface' and 'Trust Mode'. The table lists interfaces g1 through g9. Checkboxes are present next to each interface name. Interfaces g3, g5, g6, and g7 are selected (checkboxes are checked) and their rows are highlighted in yellow. The 'Trust Mode' for all interfaces is currently set to 'Disabled'.

Interface	Trust Mode
<input type="checkbox"/> g1	Disabled
<input type="checkbox"/> g2	Disabled
<input checked="" type="checkbox"/> g3	Disabled
<input type="checkbox"/> g4	Disabled
<input checked="" type="checkbox"/> g5	Disabled
<input checked="" type="checkbox"/> g6	Disabled
<input checked="" type="checkbox"/> g7	Disabled
<input type="checkbox"/> g8	Disabled
<input type="checkbox"/> g9	Disabled

3. Configure the desired settings.
4. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

➤ **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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

➤ **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 box associated with every port is selected, and the rows for all ports are highlighted.

The screenshot shows the 'Interface Configuration' page. At the top, there is a 'Go To Interface' search bar and a 'Go' button. Below this is a table with columns for 'Interface' and 'Trust Mode'. The first row is a header row with a checked checkbox, 'Interface', and 'Trust Mode'. The subsequent 16 rows represent interfaces g1 through g16, each with a checked checkbox and 'Disabled' in the Trust Mode column. The entire table is highlighted in a light yellow color.

<input checked="" type="checkbox"/>	Interface	Trust Mode
<input checked="" type="checkbox"/>	g1	Disabled
<input checked="" type="checkbox"/>	g2	Disabled
<input checked="" type="checkbox"/>	g3	Disabled
<input checked="" type="checkbox"/>	g4	Disabled
<input checked="" type="checkbox"/>	g5	Disabled
<input checked="" type="checkbox"/>	g6	Disabled
<input checked="" type="checkbox"/>	g7	Disabled
<input checked="" type="checkbox"/>	g8	Disabled
<input checked="" type="checkbox"/>	g9	Disabled
<input checked="" type="checkbox"/>	g10	Disabled
<input checked="" type="checkbox"/>	g11	Disabled
<input checked="" type="checkbox"/>	g12	Disabled
<input checked="" type="checkbox"/>	g13	Disabled
<input checked="" type="checkbox"/>	g14	Disabled
<input checked="" type="checkbox"/>	g15	Disabled
<input checked="" type="checkbox"/>	g16	Disabled

3. Configure the desired settings.
4. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

➤ **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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

➤ **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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

➤ **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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 web browser-based management interface, you can access the NETGEAR support website at www.netgear.com/support.

➤ **To access the support website from the web browser–based management 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 *Change the Default IP Address of the Switch* on page 9.

The login window opens.

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

The default password is **password**.

The Switch 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.

User Guide

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

➤ **To access the user manual online from the web browser–based management 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 *Change the Default IP Address of the Switch* on page 9.

The login window opens.

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

The default password is **password**.

The Switch 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 are given the option of registering 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>.

2. Configure System Information

2

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 you can display the switch status and specify some basic switch information, such as the management interface IP address, system clock settings, and DNS information.

This section contains the following subsections:

- [View or Define System Information and View Software Information](#) on page 29
- [Configure the Switch IP Settings](#) on page 31
- [Configure the IPv6 Network Interface](#) on page 33
- [View the IPv6 Network Neighbor](#) on page 34
- [Configure the Time Settings](#) on page 35
- [Configure Denial of Service Settings](#) on page 50
- [Configure DNS Settings](#) on page 52
- [Configure Green Ethernet Settings](#) on page 56

View or Define System Information and View Software Information

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

➤ **To view or define system information and view software 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.

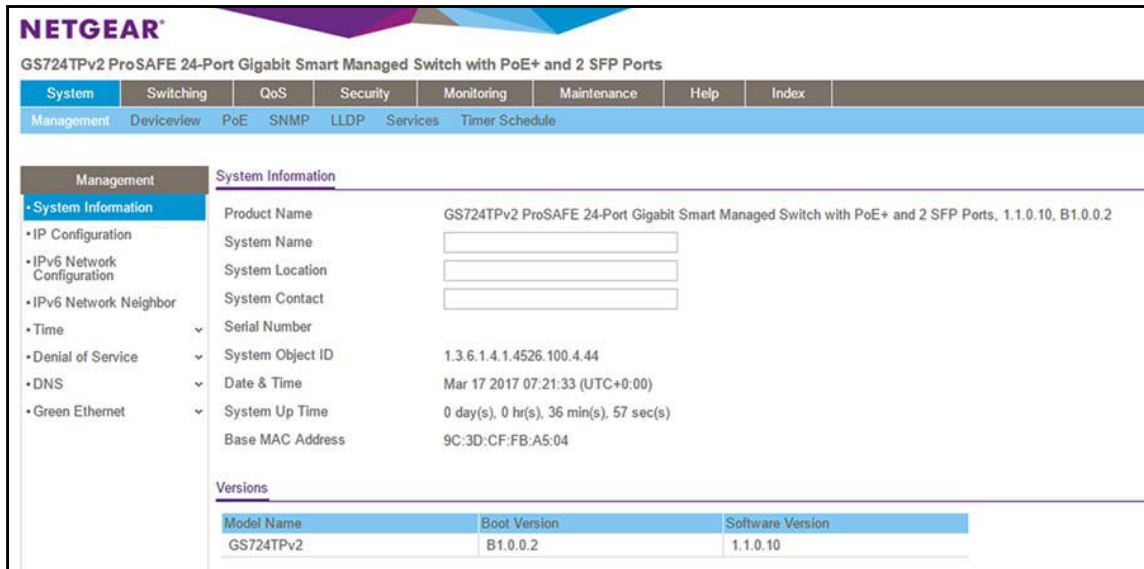
If you do not know the IP address of the switch, see [Change the Default IP Address of the Switch](#) on page 9.

The login window opens.

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

The default password is **password**.

The Switch Information page displays.



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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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

Field	Description
Product Name	The product name of this switch.
Serial Number	The serial number of the switch.
System Object OID	The base object ID for the switch's enterprise MIB.
Date & Time	The current date and time.
System Up Time	The time in days, hours, and minutes since the last switch reboot.
Base Mac Address	Universally assigned hardware address of the switch.

7. Scroll down to the Versions section.

Versions		
Model Name	Boot Version	Software Version
GS724TPv2	B1.0.0.2	1.1.0.10

- To refresh the page, click the **Update** button.

The following table describes the nonconfigurable information displayed in the Versions section of the System Information page.

Field	Description
Model Name	The model name of the switch.
Boot Version	The version of the bootloader software of the switch.
Software Version	The version number of the code currently running on the switch.

Configure the Switch IP Settings

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

➤ To configure the network information for the management interface:

- 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.

- Launch a web browser.
- 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 [Change the Default IP Address of the Switch](#) on page 9.

The login window opens.

- Enter the switch's password in the **Password** field.

The default password is **password**.

The System Information page displays.

- Select **System > Management > IP Configuration**.

The IP Configuration page displays.

- Select the appropriate radio button to specify how to configure the network information for the switch management interface:

- Dynamic IP Address (DHCP)**. Specifies that the switch must obtain the IP address through a DHCP server.

- **Dynamic IP Address (BOOTP).** Specifies that the switch must obtain the IP address through a BootP server.
 - **Static IP Address.** Specifies that the IP address, subnet mask, and default gateway must be manually configured. Enter this information in the fields below this radio button.
7. If you selected the **Static IP Address** radio button, configure the following network information:
- **IP Address.** The IP address of the network interface. The default 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 is 255.255.255.0.
 - **Default Gateway.** The default gateway for the IP interface. The default is 192.168.0.254.
8. Specify the VLAN ID for the management VLAN.

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

When the management VLAN is set to a different value, an IP connection can be made only through a port that is part of the management VLAN. 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.

Note: Make sure that the VLAN that must be the management VLAN exists. Also make sure that the PVID of at least one port in the VLAN is the same as the management VLAN ID. For information about creating VLANs and configuring the PVID for a port, see [Configure VLANs](#) on page 100.

The following requirements apply to the management VLAN:

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

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure the IPv6 Network Interface

You can configure the IPv6 network interface, which is the logical interface used for in-band connectivity with the switch through all of the switch's front-panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

To access the switch over an IPv6 network, you must initially configure the switch with IPv6 information (IPv6 prefix, prefix length, and default gateway). You can configure IPv6 using IPv6 auto-configuration option.

When in-band connectivity is established, IPv6 information can be changed using SNMP-based management or web-based management.

➤ **To configure the network information for an IPv6 network:**

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 [Change the Default IP Address of the Switch](#) on page 9.

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 > IPv6 Network Configuration**.

The IPv6 Network Global Configuration page displays.

6. Next to Admin Mode, ensure that the **Enable** radio button is selected.

7. Select the **IPv6 Address Auto Configuration Mode**.

When this mode is enabled, the network interface can acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of router advertisement messages. When this mode is disabled, the network interface does not use the native IPv6 address auto-configuration features to acquire an IPv6 address.

8. In the **IPv6 Gateway** field, specify the default gateway for the IPv6 network interface.

The gateway address is in IPv6 global or link-local address format.

9. To configure one or more static IPv6 addresses for the management interface, do the following:

- a. In the **IPv6 Prefix/Prefix Length** field, specify the static IPv6 prefix and prefix to the IPv6 network interface.

The address is in the global address format.

- b. In the **EUI64** menu, select **True** to enable the Extended Universal Identifier (EUI) flag for IPv6 address, or select **False** to omit the EUI flag.
- c. Click the **Add** button.

10. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

View the IPv6 Network Neighbor

You can view information about the IPv6 neighbors that the switch discovered through the network interface by using the Neighbor Discovery Protocol (NDP).

➤ **To view the IPv6 Network Neighbor 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 [Change the Default IP Address of the Switch](#) on page 9.

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 > IPv6 Network Neighbor**.



IPv6 Network Interface Neighbor Table				
IPv6 Address	MAC Address	isRtr	Neighbor State	Last Updated

The following table describes the information the IPv6 Network Neighbor page displays about each IPv6 neighbor that the switch discovered.

Table 4. IPv6 network interface neighbor table information

Field	Description
IPv6 address	The IPv6 address of a neighbor switch visible to the network interface.
MAC address	The MAC address of a neighbor switch.

Table 4. IPv6 network interface neighbor table information (continued)

Field	Description
IsRtr	<ul style="list-style-type: none"> • true (1). The neighbor machine is a router. • false (2). The neighbor machine is not a router.
Neighbor State	The state of the neighboring switch: <ul style="list-style-type: none"> • reachable (1). The neighbor is reachable by this switch. • stale (2). Information about the neighbor is scheduled for deletion. • delay (3). No information was received from the neighbor during the delay period. • probe (4). The switch is attempting to probe for this neighbor. • unknown (5). Unknown status.
Last Updated	The last sysUpTime that this neighbor was updated.

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 the 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Time Configuration	
Clock Source	<input checked="" type="radio"/> Local <input type="radio"/> SNTP
Date	<input type="text" value="01/03/1970"/> (MM/DD/YYYY)
Time	<input type="text" value="03:12:55"/> (HH:MM:SS)

6. Select the Clock Source **Local** radio button.
7. In the **Date** field, specify the current date in months, days, and years (MM/DD/YYYY).
8. In the **Time** field, specify the current time in hours, minutes, and seconds (HH:MM:SS).

Note: If you select the Clock Source **Local** radio button and enter information in the **Date** and **Time** fields, over a period of time, the date and time might become inaccurate. However, if you use SNTP, the date and time remain accurate (see [Configure the Time Settings With SNTP](#) on page 36 and [Configure the Global SNTP Settings](#) on page 38).

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure the Time Settings With SNTP

➤ To configure the time by using SNTP:

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 [Change the Default IP Address of the Switch](#) on page 9.

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. Next to Clock Source, select the **SNTP** radio button.

The page refreshes and displays the SNTP Global Configuration section and the SNTP Global Status section.

The default is SNTP. The local clock can be set to SNTP only if the following two conditions are met:

- The SNTP server is configured.
- The SNTP last attempt status is successful.

7. Next to Client Mode, select the mode of operation of the SNTP client:

- **Disable.** SNTP is not operational. No SNTP requests are sent from the client nor are any incoming SNTP messages processed.
- **Unicast.** SNTP operates in a point-to-point fashion. 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 is Disable.

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

For more information, see *Configure an SNTP Server* on page 42.

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 is 123. When the default is configured, the actual client port value used in SNTP packets is assigned by the OS.

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 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 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 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 is 1.

14. In the **Time Zone Name** field, specify 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 is UTC.

Note: When using SNTP/NTP time servers 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). 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 UTC.

The allowed range is -12 to 13. The default is 0.

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

The allowed range is 0 to 59. The default is 0.

17. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure the Global SNTP Settings

➤ To 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 *Change the Default IP Address of the Switch* on page 9.

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 > SNTP Global Configuration**.

When you select the **SNTP** option as the clock source, the SNTP Global Configuration section is displayed below the Time Configuration section of the page.

Management	Time Configuration
<ul style="list-style-type: none"> • System Information • IP Configuration • IPv6 Network Configuration • IPv6 Network Neighbor • Time • Time Configuration • SNTP Server Configuration • DayLight Saving Configuration • Denial of Service • DNS • Green Ethernet 	<p>Clock Source <input type="radio"/> Local <input checked="" type="radio"/> SNTP</p> <p>Date <input type="text" value="03/17/2017"/> (MM/DD/YYYY)</p> <p>Time <input type="text" value="07:36:41"/> (HH:MM:SS)</p> <hr/> <p>SNTP Global Configuration</p> <p>Client Mode <input type="radio"/> Disable <input checked="" type="radio"/> Unicast <input type="radio"/> Broadcast</p> <p>Port <input type="text" value="123"/> (123 or 1025 to 65535) Default: 123</p> <p>Unicast Poll Interval <input type="text" value="6"/> (6 to 10)</p> <p>Broadcast Poll Interval <input type="text" value="6"/> (6 to 10)</p> <p>Unicast Poll Timeout <input type="text" value="5"/> (1 to 30)</p> <p>Unicast Poll Retry <input type="text" value="1"/> (0 to 10)</p> <p>Time Zone Name <input type="text"/></p> <p>Offset Hours <input type="text" value="0"/> (-12 to 13)</p> <p>Offset Minutes <input type="text" value="0"/> (0 to 59)</p>

6. Select a **Client mode** radio button to specify the mode of operation of the SNTP client:
- **Disable.** SNTP is not operational. No SNTP requests are sent from the client and no received SNTP messages are processed.
 - **Unicast.** SNTP operates in a point-to-point fashion. 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 is Unicast.

7. 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 the value 123. The default is 123. When the default is configured, the actual client port value used in SNTP packets is assigned by the operating system.
8. 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 is 6.
9. 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 is 6.
10. 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 is 5.

11. 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 is 1.

12. In the **Time Zone Name** field, specify 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 is UTC.

Note: When using SNTP/NTP time servers 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). This might not be the time zone in which the switch is located.

13. In the **Offset Hours** field, specify the number of hours that the time zone is different from UTC.

The allowed range is -12 to 13. The default is 0.

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

The allowed range is 0 to 59. The default is 0.

15. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

16. To refresh the page, click the **Update** button.

View SNTP Global Status

When you select the **SNTP** option as the clock source, the SNTP global status is displayed below the SNTP Global Configuration section of the page. The SNTP Global Status table displays information about the system's SNTP client.

➤ To view 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 [Change the Default IP Address of the Switch](#) on page 9.

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 > SNTP Global Status.**

When you select the **SNTP** option as the clock source, the SNTP Global Status is displayed below the SNTP Global Configuration section.

SNTP Global Status	
Version	4
Supported Mode	Unicast and Broadcast
Last Update Time	Mar 17 07:36:31 2017 (UTC+0:00)
Last Attempt Time	Mar 17 07:36:30 2017 (UTC+0:00)
Last Attempt Status	Success
Server IP Address	172.16.167.54
Address Type	IPv4
Server Stratum	3 - Secondary Reference
Reference Clock Id	NTP Srv: 173.255.215.209
Server Mode	Server
Unicast Server Max Entries	3
Unicast Server Current Entries	1
Broadcast Count	0

6. Click the **Update** button to update the page with the latest information about the switch.

The following table displays the nonconfigurable information on the page.

Table 5. SNTP Global Status information

Field	Description
Version	The SNTP version that the client supports.
Supported mode	The SNTP modes that the client supports. Multiple modes can be supported by a client.
Last Update Time	The local date and time (UTC) that the SNTP client last updated the system clock.
Last Attempt Time	The local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.

Table 5. SNTP Global Status information (continued)

Field	Description
Last Attempt Status	<p>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.</p> <ul style="list-style-type: none"> • 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.
Server Stratum	The claimed stratum of the server for the last received valid packet.
Reference Clock ID	The reference clock identifier of the server for the last received valid packet.
Server mode	The mode of the server for the last received valid packet.
Unicast Server Max Entries	The maximum number of unicast server entries that can be configured on this client.
Unicast Server Current Entries	The number of current valid unicast server entries configured for this client.
Broadcast Count	The number of unsolicited broadcast SNTP messages that were received and processed by the SNTP client since the last reboot.

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 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

SNTP Server Configuration				
Server Type	Address	Port	Priority	Version
<input type="checkbox"/> ▼				

SNTP Server Status					
Address	Last Update Time	Last Attempt Time	Last Attempt Status	Requests	Failed Requests

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, IPv6) or a host name (DNS). The default is IPv4.
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 valid range is 1 to 65535. The default is 123.
9. In **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 valid range is 1 to 3. The default is 1.
10. In the **Version** field, specify the NTP version running on the server. The range is 1 to 4. The default is 4.
11. Click the **Add** button. The SNTP server entry is added. This sends the updated configuration to the switch. Configuration changes take effect immediately.
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 fields in the SNTP Server Status table.

Table 6. SNTP Server Status information

Field	Description
Address	All the existing server addresses. If no server configuration exists, a message stating that no SNTP server exists displays on the page.
Last Update Time	The local date and time (UTC) that the response from this server was used to update the system clock.
Last Attempt Time	The local date and time (UTC) that this SNTP server was last queried.
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: <ul style="list-style-type: none"> • Other. The status of the last request is unknown, or no SNTP responses were received. • 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 on 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.
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.

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 [Change the Default IP Address of the Switch](#) on page 9.

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.

8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 [Change the Default IP Address of the Switch](#) on page 9.

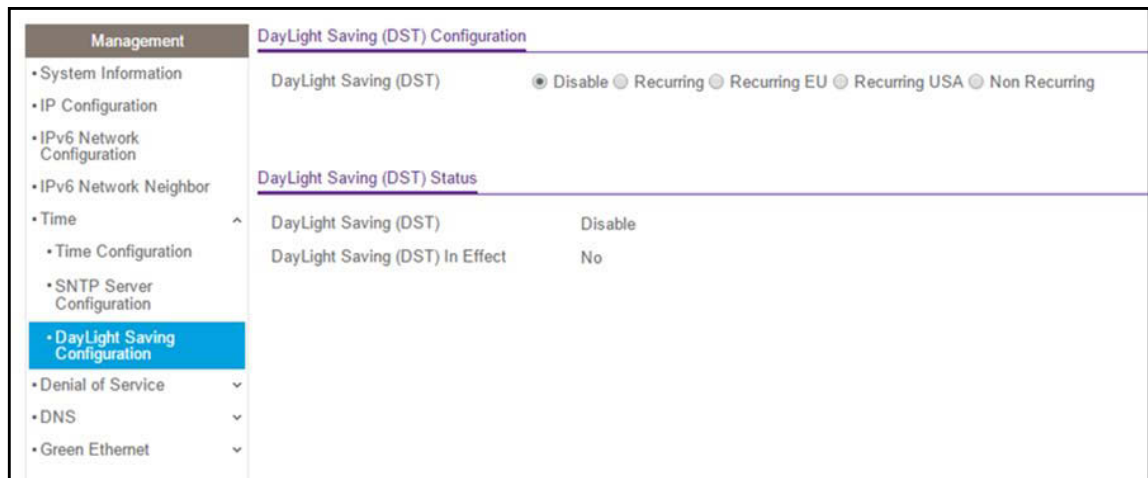
The login window opens.

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**.



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. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The fields that are described in the following table are visible on the page only if the DayLight Saving (DST) **Recurring**, **Recurring EU**, or **Recurring USA** radio button is selected.

Table 7. Daylight saving setting is Recurring, Recurring EU, or Recurring USA

Field	Description
Begins At	These fields are used to configure the start values of the date and time. <ul style="list-style-type: none"> • Week. Configure the start week. • Day. Configure the start day. • Month. Configure the start month. • Hours. Configure the start hours. • Minutes. Configure the start minutes.
Ends At	These fields are used to configure the end values of date and time. <ul style="list-style-type: none"> • Week. Configure the end week. • Day. Configure the end day. • Month. Configure the end month. • Hours. Configure the end hours. • Minutes. Configure the end minutes.
Offset	Configure recurring offset in minutes. The valid range is 1–1440 minutes.
Zone	Configure the time zone.

The fields that are described in the following table are visible on the page only if the DayLight Saving (DST) **Non Recurring** radio button is selected.

Table 8. Daylight saving setting is Non Recurring

Field	Description
Begins At	These fields are used to configure the start values of the date and time. <ul style="list-style-type: none"> • Week. Configure the start week. • Day. Configure the start day. • Month. Configure the start month. • Hours. Configure the start hours. • Minutes. Configure the start minutes.
Ends At	These fields are used to configure the end values of date and time. <ul style="list-style-type: none"> • Week. Configure the end week. • Day. Configure the end day. • Month. Configure the end month. • Hours. Configure the end hours. • Minutes. Configure the end minutes.

Table 8. Daylight saving setting is Non Recurring (continued)

Field	Description
Offset	Specify the number of minutes to shift the summer time from the standard time. The valid range is 1–1440 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.

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

The screenshot shows the web interface for configuring DayLight Saving (DST). On the left, a navigation menu lists various system settings, with 'DayLight Saving Configuration' highlighted in blue. The main content area is titled 'DayLight Saving (DST) Configuration'. It features a section for 'DayLight Saving (DST)' with radio buttons for 'Disable' (selected), 'Recurring', 'Recurring EU', 'Recurring USA', and 'Non Recurring'. Below this is a section titled 'DayLight Saving (DST) Status' which displays two rows: 'DayLight Saving (DST)' with a value of 'Disable', and 'DayLight Saving (DST) In Effect' with a value of 'No'.

6. To refresh the page, click the **Update** button.

The following table displays the nonconfigurable information on the page.

Table 9. Daylight Saving (DST) Status information

Field	Description
Daylight Saving (DST)	The Daylight Saving value, which is one of the following: <ul style="list-style-type: none"> • Disable • Recurring • Recurring EU • Recurring USA • Non Recurring
Begins At	Displays when the daylight saving time begins. This field is not displayed when daylight saving time is disabled.
Ends At	Displays when the daylight saving time ends. This field is not displayed when daylight saving time is disabled.
Offset (in Minutes)	The offset value in minutes. This field is not displayed when daylight saving time is disabled.
Zone	The zone acronym. This field is not displayed when daylight saving time is disabled.
Daylight Saving (DST) in Effect	Displays whether daylight saving time is in effect.

Configure Denial of Service Settings

You can configure Denial of Service (DoS), allowing the switch to classify and block specific types of DoS attacks.

Configure Auto-DoS

The Auto-DoS Configuration page lets you 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 51.

➤ **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 [Change the Default IP Address of the Switch](#) on page 9.

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. Next to Auto-DoS Mode, select the **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.

7. Click the **Apply** button.

The updated configuration is sent to the switch, and configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

The screenshot shows the 'Denial of Service Configuration' page. It contains four rows of settings:

Denial of Service Configuration	
Denial of Service ICMPv4	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Denial of Service Max ICMPv4 Packet Size	<input type="text" value="512"/> (0 to 1023)
Denial of Service ICMPv6	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Denial of Service Max ICMPv6 Packet Size	<input type="text" value="512"/> (0 to 1023)

6. Select the types of DoS attacks for the switch to monitor and block and configure any associated values:
 - **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.
 - **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 IPv6 ICMP packet size allowed. If ICMPv6 DoS prevention is enabled, the switch drops IPv6 ICMP ping packets with a size greater than the configured maximum ICMPv6 packet size.
7. Click the **Apply** button.

The updated configuration is sent to the switch, and configuration changes take effect immediately.

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

You can configure global DNS settings and DNS server information.

➤ To configure the global DNS 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

ID	DNS Server	Preference
1	10.130.2.20	1
2	10.136.124.1	2

6. Select the **Disable** or **Enable** radio button to specify whether to disable or enable the administrative status of the DNS client.
 - **Enable.** Allow the switch to send DNS queries to a DNS server to resolve a DNS domain name. The DNS is enabled by default.
 - **Disable.** Prevent 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 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. To remove a DNS server from the list, select its check box and click the **Delete** button.

If you click the **Delete** button without selecting a DNS server, all the DNS servers are deleted.

11. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

12. To refresh the page, click the **Update** button.

The following table describes the fields that are shown in the DNS Server Configuration table.

Table 10. DNS Server Configuration information

Field	Description
ID	The identification of the DNS Server.
Preference	Shows the preference of the DNS server. The preferences are determined by the order in which they were entered.

Configure and View Host Name-to-IP Address Information

You can manually map host names to IP addresses and 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

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.

The entry displays in the list on the page.

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 [Change the Default IP Address of the Switch](#) on page 9.

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.

Change the Host Name or IP Address in an Entry of the Dynamic Host Mapping Table and View All Entries

➤ **To change the host name or IP address in an entry of the dynamic host mapping table and view 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 [Change the Default IP Address of the Switch](#) on page 9.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 11. Dynamic Host Mapping information

Field	Description
Host	Lists the host name that you assign to the specified IP address.
Total	Time since the dynamic entry was first added to the table.
Elapsed	Time since the dynamic entry was last updated.
Type	The type of the dynamic entry.
Addresses	Lists the IP address associated with the host name.

Configure Green Ethernet Settings

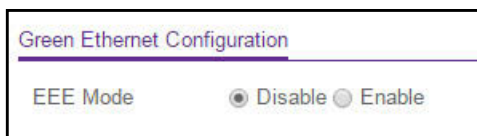
Using the Green Ethernet feature allows for power consumption savings.

Configure Green Ethernet Global Settings

You can configure Green Ethernet features.

➤ 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 [Change the Default IP Address of the Switch](#) on page 9.
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 EEE Mode **Disable** or **Enable** radio button.

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 IEEE 802.3az Energy Efficient Task Force. Lower power mode enables both the send and receive sides of the link to disable some functionality for power savings when lightly loaded. 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.

7. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure Green Ethernet Interface Settings

You can configure per-port Green Ethernet settings.

➤ 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Green Ethernet Interface Configuration

1 Go To Interface

<input type="checkbox"/>	Port	EEE Mode
<input type="checkbox"/>	g1	Disabled
<input type="checkbox"/>	g2	Disabled
<input type="checkbox"/>	g3	Disabled
<input type="checkbox"/>	g4	Disabled
<input type="checkbox"/>	g5	Disabled
<input type="checkbox"/>	g6	Disabled
<input type="checkbox"/>	g7	Disabled
<input type="checkbox"/>	g8	Disabled
<input type="checkbox"/>	g9	Disabled

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 (for example, g1) 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 **EEE mode** menu, select **Enable** or **Disable**.
The default is Disable.
8. Click the **Apply** button.
The updated configuration is sent to the switch. Configuration changes take effect immediately.

Use the Device View

For device view information, see [Web Browser–Based Management Interface Device View](#) on page 19.

Configure PoE

The switch can supply up to 30W PoE+ (IEEE 802.3at) to each port, with a maximum PoE power budget of 190W across all active PoE+ ports.

By default, supplied power is prioritized according to the port order, up to the total power budget of the device. Port 1 receives the highest PoE priority, while port 24 is relegated to the lowest PoE priority.

If the power requirements for attached devices exceed the total power budget of the switch, the PoE power to the device on the highest-numbered active PoE port is disabled to make

sure that the devices connected to the higher-priority, lower-numbered PoE ports are supported first.

Although a device is listed as an 802.3at PoE+-powered or 802.3af PoE-powered device, it might not require the maximum power limit that is specified by its IEEE standard. Many devices require less power, allowing all 24 PoE ports to be active simultaneously when the devices correctly report their PoE class to the switch.

Configure PoE Trap Settings and View PoE Information

You can configure the PoE trap settings and view PoE information such as nominal power, threshold power, and consumed power.

➤ To configure the PoE trap settings and view PoE 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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Basic > PoE Configuration**.

PoE Configuration						
<input type="checkbox"/>	Firmware Version	Power Status	Nominal Power	Threshold Power	Consumed Power	Traps
<input checked="" type="checkbox"/>	1.8.0.B5	ON	190 Watt	183 Watt	7.2 Watt	Enable

6. From the **Traps** menu, select **Enable** or **Disable**.

The default is Enable. Selecting **Disable** deactivates the PoE traps.

7. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable fields on the page.

Table 12. PoE Configuration fields

Field	Description
Firmware Version	The firmware version of the PoE firmware component.
Power Status	The power status.
Nominal Power	The maximum amount of power in watts that the switch can deliver to all ports.
Threshold Power Watts	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.
Consumed Power Watts	The total amount of power in watts that is being delivered to all ports.

Configure the PoE Port Settings

You can configure PoE settings for individual PoE ports.

➤ **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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Port	Admin Mode	High Power	Max Power	Priority Level	High Power Mode	Detection Mode	Class	Timer Schedule	Output Voltage (Volt)	Output Current (mA)	Output Power (Watt)	Power Limit Type	Power Limit (mWatt)
g1	Enable	Yes	30000	Low	802.3at	ieee	0	test	53	136	7.3	Class	30000
g2	Enable	Yes	30000	Low	802.3at	ieee	0	None	0	0	0.0	Class	30000
g3	Enable	Yes	30000	Low	802.3at	ieee	0	None	0	0	0.0	Class	30000
g4	Enable	Yes	30000	Low	802.3at	ieee	0	None	0	0	0.0	Class	30000
g5	Enable	Yes	30000	Low	802.3at	ieee	0	None	0	0	0.0	Class	30000
g6	Enable	Yes	30000	Low	802.3at	ieee	0	None	0	0	0.0	Class	30000
g7	Enable	Yes	30000	Low	802.3at	ieee	0	None	0	0	0.0	Class	30000
g8	Enable	Yes	30000	Low	802.3at	ieee	0	None	0	0	0.0	Class	30000

6. Select one or more ports by taking one of the following actions:
 - To configure a single port, select the check box associated with the port, or type the port number (for example, g1) in the **Go To Interface** field and click the **Go** button.
 - To configure multiple ports with the same settings, select the check box associated with each interface.
 - To configure all ports with the same settings, select the check box in the heading row.
7. From the **Admin Mode** menu, select the administrative 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 **High 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 **Detection Type** menu, select how the port detects the attached PD:
 - **pre-ieee**. The port performs legacy detection.
 - **ieee auto**. The port performs a 4-point resistive detection. This is the default setting.
 - **auto**. The port performs a 4-point resistive detection, and if required, continues with legacy detection.
11. 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 87.

12. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable fields on the page.

Table 13. PoE Port Configuration

Field	Description
High Power	All ports supports high-power mode.
Max Power	The maximum power in milliwatts that can be provided by the port.
Class	The class defines the range of power that a powered device (PD) is drawing from the switch. The class definitions are as follows: <ul style="list-style-type: none"> • 0: 0.44–12.95W • 1: 0.44–3.83W • 2: 0.44–6.48W • 3: 0.44–12.95W • 4: 0.44–25.5W
Output Voltage	The voltage that is delivered to the PD in volts.
Output Current	The current that is delivered to the PD in mA.
Output Power	The power that is delivered to the PD in watts.
Status	The operational status of the port. The possible values are as follows: <ul style="list-style-type: none"> • Disabled. No power is delivered. • DeliveringPower. Power is being drawn by the PD. • Fault. A problem occurred with the power. • Test. The port is in test mode. • otherFault. The port is idle because of an error condition. • Searching. The port is not in one of the other states in this list.
Fault Status	The error description when the PoE port is in a fault state. The possible values are as follows: <ul style="list-style-type: none"> • No Error. The port is not in any error state and can provide power. • MPS Absent. The port detected the absence of the main power supply, preventing the port from providing power. • Short. The port detected a short circuit condition, preventing the port from providing power. • Overload. The PD that is connected to the port attempts to draw more power than allowed by the port's settings, preventing the port from providing power at all. • Power Denied. The port was denied power because of a shortage of power or because of an administrative condition. In this condition, the port cannot provide power.

Configure SNMP

You can configure SNMP settings for SNMPv1/v2 and SNMPv3. The switch 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. The main object for interface configuration is in NetgearSmartSwitch-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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Community Configuration					
<input type="checkbox"/>	Management Station IP	Management Station IP Mask	Community String	Access Mode	Status
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	0.0.0.0	0.0.0.0	public	ReadOnly	Enable

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 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 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 parameters are 192.168.1.0/255.255.255.0, any client with an IP address from one 192.168.1.0 through 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 machine's IP address for 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 [Change the Default IP Address of the Switch](#) on page 9.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Recipients IP	Version	Community String	Status
<input type="text"/>	SNMP V1	<input type="text"/>	Disable

6. In the **Recipients IP** field, enter the IPv4 address in the x.x.x.x format to receive SNMP traps from this device.
7. From the **Version** menu, select the trap version to be used by the SNMP trap receiver.
 - **SNMP V1**. The switch uses SNMPv1 to send traps to the receiver. The default setting is **SNMP V1**.
 - **SNMP V2**. 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 [Change the Default IP Address of the Switch](#) on page 9.

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. Update the desired fields.
8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 [Change the Default IP Address of the Switch](#) on page 9.

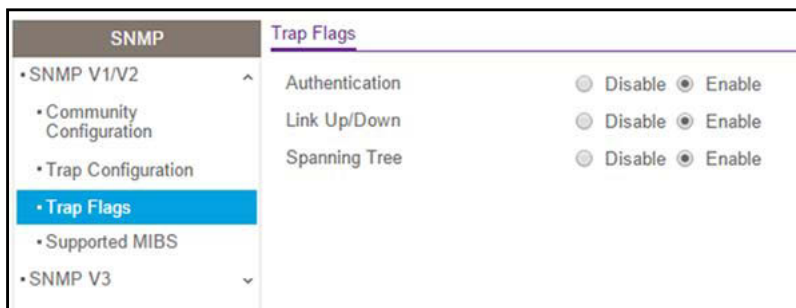
The login window opens.

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**.



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 device management interface and fails to 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.

7. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

View the Supported MIBs

You can view a list of all MIBs that are supported by 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Status	
Name	Description
RFC 1907 - SNMPv2-MIB	The MIB module for SNMPv2 entities
HC-RMON-MIB	The original version of this MIB, published as RFC3273.
HENUM-TC	A MIB module containing textual conventions for high capacity data types.
SNMP-COMMUNITY-MIB	This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2, and SNMPv3.
SNMP-MPD-MIB	The MIB for Message Processing and Dispatching
SNMP-TARGET-MIB	The Target MIB Module
SNMP-VIEW-BASED-ACM-MIB	The management information definitions for the View-based Access Control Model for SNMP.
NETGEAR-UDLD-MIB	UDLD MIB

The following table describes the nonconfigurable information on the page.

Table 14. SNMP supported MIBs

Field	Description
Name	The RFC number if applicable and the name of the MIB.
Description	The RFC title or MIB description.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 is a read-only field that 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](#) on page 179.

7. To enable encryption:

- a. Next to Encryption Protocol, select the **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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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. This information is viewed by a network manager to identify system topology and detect bad configurations on the LAN.

This section contains the following subsections:

- [Configure LLDP Global Settings](#) on page 71
- [Configure LLDP Port Settings](#) on page 73
- [View LLDP-MED Network Policy Information](#) on page 74
- [Configure LLDP-MED Port Settings](#) on page 76
- [View Local LLDP Information](#) on page 77
- [View LLDP Neighbors Information](#) on page 79

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 enabled 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 parameters 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

LLDP	
• Basic	^
• LLDP Configuration	•
• Advanced	^

LLDP Properties	
TLV Advertised Interval	30 (5 to 32768 secs)
Hold Multiplier	4 (2 to 10 secs)
Reinitializing Delay	2 (1 to 10 secs)
Transmit Delay	5 (5 to 3600 secs)

LLDP-MED Properties	
Fast Start Duration	3 (1 to 10 Times)

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 × 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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Interface	Admin Status	Management IP Address	Notification	Optional TLVs
<input type="checkbox"/> g1	Tx and Rx	Auto Advertise	Disable	Enable
<input type="checkbox"/> g2	Tx and Rx	Auto Advertise	Disable	Enable
<input type="checkbox"/> g3	Tx and Rx	Auto Advertise	Disable	Enable
<input type="checkbox"/> g4	Tx and Rx	Auto Advertise	Disable	Enable
<input type="checkbox"/> g5	Tx and Rx	Auto Advertise	Disable	Enable
<input type="checkbox"/> g6	Tx and Rx	Auto Advertise	Disable	Enable
<input type="checkbox"/> g7	Tx and Rx	Auto Advertise	Disable	Enable
<input type="checkbox"/> g8	Tx and Rx	Auto Advertise	Disable	Enable
<input type="checkbox"/> g9	Tx and Rx	Auto Advertise	Disable	Enable
<input type="checkbox"/> g10	Tx and Rx	Auto Advertise	Disable	Enable

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 TLV(s).** 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 29. For information about how to configure the port description, see [Configure Port Settings](#) on page 93.

8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

View LLDP-MED Network Policy Information

You can display information about the LLDP-MED network policy TLVs 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 [Change the Default IP Address of the Switch](#) on page 9.

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.

The page refreshes and displays the data transmitted in the network policy TLVs for the interface.

The following table describes nonconfigurable information on the page.

Table 15. LLDP-MED network policy information

Field	Description
Network Policy Number	The policy number.
Application	<p>The media application type associated with the policy, which can be one of the following:</p> <ul style="list-style-type: none"> • Unknown • Voice • Guest Voice • Guest Voice Signaling • Softphone Voice • Video Conferencing • Streaming Video • Video Signaling <p>A port can receive multiple application types. The application information is displayed only if a network policy TLV was transmitted from the port.</p>
VLAN ID	The VLAN ID associated with the policy.
VLAN Type	Indicates whether the VLAN associated with the policy is tagged or untagged.
User Priority	The priority associated with the policy.
DSCP	The DSCP associated with a particular policy type.

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 [Change the Default IP Address of the Switch](#) on page 9.

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.
- **Transmit Optional TLVs.** When Transmit Optional TLVs is enabled, the port transmits the following optional type length values (TLVs) in the LLDP PDU frames:
 - MED Capabilities
 - Network Policy
 - Location Identification
 - Extended Power via MDI: PSE
 - Extended Power via MDI: PD
 - Inventory

8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

View Local LLDP Information

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

LLDP		Device Information			
• Basic	Chassis ID Subtype	MAC Address			
• Advanced	Chassis ID	9C:3D:CF:FB:A5:04			
• LLDP Configuration	System Name	ttt			
• LLDP Port Settings	System Description	GS724TPv2			
• LLDP-MED Network Policy	System Capabilities	bridge			
• LLDP-MED Port Settings	Port Information				
• Local Information	Interface	Port ID Subtype	Port ID	Port Description	Advertisement
• Neighbors Information	g1	Interface Name	e1		Enable
	g2	Interface Name	e2		Enable
	g3	Interface Name	g1		Enable
	g4	Interface Name	g2		Enable
	g5	Interface Name	g3		Enable
	g6	Interface Name	g4		Enable
	g7	Interface Name	g5		Enable

The page includes only the interfaces on which LLDP is enabled.

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

Field	Description
Chassis ID Subtype	The type of information used to identify the switch in the Chassis ID field.
Chassis ID	The hardware platform identifier for the switch.
System Name	The user-configured system name for the switch.
System Description	The switch description, which includes information about the product model and platform.

Field	Description
System Capabilities	The primary functions that the switch supports.
Interface	The interface associated with the rest of the data in the row.
Port ID Subtype	The type of information used to identify the interface in the Port ID field.
Port ID	The port number.
Port Description	The user-defined description of the port. For information about how to configure the port description, see Configure Port Settings on page 93.
Advertisement	The TLV advertisement status of the port.

6. 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.

Field	Description
Managed Address	
Address SubType	The type of address the management interface uses, such as an IPv4 address.
Address	The address used to manage the device.
Interface SubType	The port subtype.
Interface Number	The number that identifies the port.
MAC/PHY Details	
Auto Negotiation Supported	Indicates whether the interface supports port speed autonegotiation. The possible values are True and False.
Auto Negotiation Enabled	The port speed autonegotiation support status. The possible values are True (enabled) or False (disabled).
Auto Negotiation Advertised Capabilities	The port speed autonegotiation capabilities such as 100BASE-T half-duplex mode or 10BASE-TX full-duplex mode.
Operational MAU Type	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.
MED Details	
Capabilities Supported	The MED capabilities enabled on the port.
Current Capabilities	The TLVs advertised by the port.
Device Class	Network Connectivity indicates that the device is a network connectivity device.

Field	Description
Network Policies	
Application Type	The media application type associated with the policy.
VLAN ID	The VLAN ID associated with the policy.
VLAN Type	Specifies whether the VLAN associated with the policy is tagged or untagged.
User Priority	The priority associated with the policy.
DSCP	The DSCP associated with a particular policy type.

View LLDP Neighbors Information

You can view the data that a specific interface receives 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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Neighbor Information**.

MSAP Entry	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name
------------	------------	--------------------	------------	-----------------	---------	-------------

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

The following table describes the information that displays for all LLDP neighbors that were discovered.

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

- 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.

Field	Description
Port Details	
Local Port	The interface on the local system that received LLDP information from a remote system.
MSAP Entry	The Media Service Access Point (MSAP) entry number for the remote device.
Basic Details	
Chassis ID Subtype	The type of data displayed in the Chassis ID field on the remote system.
Chassis ID	The remote 802 LAN device's chassis.
Port ID Subtype	The type of data displayed in the remote system's Port ID field.
Port ID	The physical address of the port on the remote system from which the data was sent.
Port Description	The user-defined description of the port.
System Name	The system name associated with the remote device.
System Description	The description of the selected port associated with the remote system.
System Capabilities	The system capabilities of the remote system.

Field	Description
Managed Addresses	
Address SubType	The type of the management address.
Address	The advertised management address of the remote system.
Interface SubType	The port subtype.
Interface Number	The port on the remote device that sent the information.
MAC/PHY Details	
Auto-Negotiation Supported	Specifies whether the remote device supports port-speed autonegotiation. The possible values are True or False.
Auto-Negotiation Enabled	The port speed autonegotiation support status. The possible values are True and False.
Auto Negotiation Advertised Capabilities	The port speed autonegotiation capabilities.
Operational MAU Type	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.
MED Details	
Capabilities Supported	The supported capabilities that were received in MED TLV from the device.
Current Capabilities	The advertised capabilities that were received in MED TLV from the device.
Device Class	The LLDP-MED endpoint device class. The possible device classes are as follows: <ul style="list-style-type: none"> Endpoint Class 1 Indicates a generic endpoint class, offering basic LLDP services. Endpoint Class 2 Indicates a media endpoint class, offering media streaming capabilities as well as all Class 1 features. Endpoint Class 3 Indicates a communications device class, offering all Class 1 and Class 2 features plus location, 911, Layer 2 switch support, and device information management capabilities.
Hardware Revision	The hardware version advertised by the remote device.
Firmware Revision	The firmware version advertised by the remote device.
Software Revision	The software version advertised by the remote device.
Serial Number	The serial number advertised by the remote device.
Model Name	The model name advertised by the remote device.
Asset ID	The asset ID advertised by the remote device.

Field	Description
Location Information	
Civic	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.
Coordinates	The location map coordinates that the remote device advertised in the location TLV, including latitude, longitude, and altitude.
ECS ELIN	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.
Unknown	Displays unknown location information for the remote device.
Network Policies	
Application Type	The media application type associated with the policy advertised by the remote device.
VLAN ID	The VLAN ID associated with the policy.
VLAN Type	Specifies whether the VLAN associated with the policy is tagged or untagged.
User Priority	The priority associated with the policy.
DSCP	The DSCP associated with a particular policy type.
LLDP Unknown TLVs	
Type	The unknown TLV type field.
Value	The unknown TLV value field.

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.

If you do not know the IP address of the switch, see [Change the Default IP Address of the Switch](#) on page 9.

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**.

Services		DHCP Snooping Global Configuration	
• DHCP Snooping	▼	DHCP Snooping Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
• Global Configuration		MAC Address Validation	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
• Interface Configuration		VLAN Configuration	
• Binding Configuration		VLAN ID	DHCP Snooping Mode
		<input type="text"/>	<input type="text"/>

6. Next to DHCP Snooping Mode, select the **Enable** radio button.
7. To enable the verification of the sender's MAC address for DHCP snooping, next to MAC Address Validation, select the **Enable** radio button.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.
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.
The updated configuration is sent to the switch. Configuration changes take effect immediately.

Interface Configuration

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.

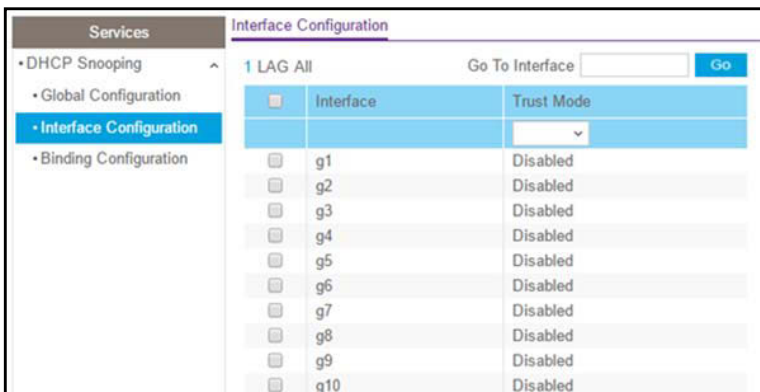
➤ To configure DHCP snooping interface settings:

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 [Change the Default IP Address of the Switch](#) on page 9.
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 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 **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 (DHCP OFFER, DHCP ACK, DHCP NAK, DHCP RELEASE QUERY) are dropped.
 - DHCP RELEASE and DHCP DECLINE 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.

8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Binding Configuration

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

➤ To configure 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Interface	MAC Address	VLAN ID	IP Address

Interface	MAC Address	VLAN ID	IP Address	Lease Time

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 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.

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 16. DHCP Dynamic Configuration information

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

Set Up PoE Timer Schedules

The switch lets you define multiple timer schedules 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 60). 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.

Create a PoE Timer Schedule

The maximum number of timer schedules that you can add is 25.

➤ 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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Timer Global Configuration**.

Timer Schedule

Admin Mode Disable Enable

Timer Schedule Name

Timer Schedule Name	ID
test	1

6. Select the Admin Mode **Enable** radio button.
By default, the Disable button is selected and PoE timer schedules are disabled.
7. In the **Timer Schedule Name** field, specify the name for a timer schedule.
8. Click the **Add** button.
The timer schedule is added to the Timer Schedule Name table and is assigned an ID.

Specify the Settings for a PoE Timer Schedule

The PoE timer schedule functions as a recurring schedule, which lets you to set up a single schedule that starts at a particular date and that recurs either with a specific end date or indefinitely.

You can specify a daily, weekly, monthly, or yearly recurring schedule.

➤ To specify the settings for 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 [Change the Default IP Address of the Switch](#) on page 9.
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**.

Timer Schedule Selection	
Timer Schedule Name	test
Timer Schedule Configuration	
Shutdown Time Start	09:11 (hh:mm)
Shutdown Time End	09:12 (hh:mm)
Date Start	17-Mar-2017
Date Stop	<input type="radio"/> No End Date <input checked="" type="radio"/> End Date 18-Mar-2017
Recurrence Pattern	Daily
Daily Mode	<input checked="" type="radio"/> Every WeekDay <input type="radio"/> Every Day(s)

6. From the **Timer Schedule Name** menu, 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 87).

7. In the **Shutdown Time Start** field, enter the time of day in the HH:MM format to specify when the timer schedule must start.
8. In the **Shutdown Time End** field, enter the time of day in the HH:MM format to specify when the timer schedule must stop.
9. 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-YYYY format to specify when the timer schedule must start.
10. 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-YYYY format to specify when the timer schedule must stop.
11. From the **Recurrence Pattern** menu, select the pattern:
- **Daily.** The timer schedule works with daily recurrence. The fields adjust. Select one of the following radio buttons:
 - **Every WeekDay.** The schedule operates from Monday through Friday.
 - **Every Day(s).** Enter a number from 0 to 65534 in the field. 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. Specify the following field and select one or more of the following check boxes:
 - **Every Week(s).** In the field, enter a number from 0 to 65534 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. Select one of the following radio buttons:
 - Upper **Day** radio button and field. 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 65534 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.

- Lower **Day** radio button and field. Select an option from both the left menu and right menu.

In the **Every Month(s)** field, enter a number from 0 to 65534 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.

- **Yearly.** The timer schedule works with yearly recurrence. The fields adjust. Select one of the following radio buttons:

- **Day(s).** In the **Day(s)** field, enter a number from 1 to 31 to specify the day of the month when the schedule must be triggered.

From the **Month** menu, select the month in which the schedule must be triggered. The schedule is triggered yearly but only in the selected month.

- **Day(s).** Select an option from both the left menu and right menu.

From the **Month** menu, select the month in which the schedule must be triggered. The schedule is triggered yearly but only in the selected month.

12. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Delete a PoE Timer Schedule

You can delete a PoE timer schedule that you no longer need. The associated timer schedule configuration is 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 [Change the Default IP Address of the Switch](#) on page 9.

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 Global Configuration**.

The Timer Schedule Configuration page displays.

6. Select the check box for the timer schedule that you want to delete.

You can simultaneously delete multiple or all timer schedules.

7. Click the **Delete** button.

The timer schedule is deleted.

3. Configure Switching

3

This chapter contains the following sections:

- *Configure Port Settings*
- *Configure Link Aggregation Groups*
- *Configure VLANs*
- *Configure a Voice VLAN*
- *Configure Auto-VoIP*
- *Configure Spanning Tree Protocol*
- *Configure Multicast*
- *View and Configure the MAC Address Table*

Configure Port Settings

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

➤ To configure 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

The following figure that does not display all columns of the table.

Port	Description	Port Type	Admin Mode	Auto-negotiation	Speed	Duplex Mode	Auto Power Down Mode	Physical Status	Link Status	Link Trap	Frame Size (1518 to 9216)	Flow Control	MAC Address
<input type="checkbox"/> g1			Enable	Enable	Auto	Auto	Disable		Link Down	Enable	1518	Disable	9C:3D:CF:FB:A5:00
<input type="checkbox"/> g2			Enable	Enable	Auto	Auto	Disable		Link Down	Enable	1518	Disable	9C:3D:CF:FB:A5:00
<input type="checkbox"/> g3			Enable	Enable	Auto	Auto	Disable		Link Down	Enable	1518	Disable	9C:3D:CF:FB:A5:00
<input type="checkbox"/> g4			Enable	Enable	Auto	Auto	Disable		Link Down	Enable	1518	Disable	9C:3D:CF:FB:A5:00
<input type="checkbox"/> g5			Enable	Enable	Auto	Auto	Disable		Link Down	Enable	1518	Disable	9C:3D:CF:FB:A5:00
<input type="checkbox"/> g6			Enable	Enable	Auto	Auto	Disable		Link Down	Enable	1518	Disable	9C:3D:CF:FB:A5:00

6. Select the check box to the left of the Port column to specify the interface for which data is to be displayed or configured.

To select an interface, you can also enter the interface number in the **Go To Interface** field and click the **Go** button.

7. In the **Description** field, enter the description string to be attached to a port.

The string can be up to 64 characters in length.

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

This sets the port control administrative mode. You must select **Enable** in order for the port to participate in the network. The default is Enable.

9. From the **Auto-negotiation** menu, select **Enable** or **Disable**.

This specifies the autonegotiation mode for this 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.

10. In the **Speed** field, specify the speed value for the selected port.

Possible field values are as follows:

- **Auto.** All supported speeds. This is the default setting.
- **10Mbps.** 10 Mbits/second.
- **100Mbps.** 100 Mbits/second.
- **1000Mbps.** 1000 Mbits/second.

The delimiter characters for setting different speed values are a comma (,), a period (.) and a space (.). For you to set the auto-negotiation 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.

11. From the **Duplex Mode** menu, select the duplex mode for the selected port.

Possible values are as follows:

- **Auto.** Indicates that speed is set by the auto-negotiation process.
- **Full.** Indicates that the interface supports transmission between the devices in both directions simultaneously.
- **Half.** Indicates that the interface supports transmission between the devices in only one direction at a time.

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.

12. From the **Auto Power Down Mode** menu, select whether the auto power down mode of the Green Ethernet feature is enabled or disabled.

The default is disabled.

13. Use the **Link Trap** menu to select whether to send a trap when link status changes.

The default is enabled for normal interfaces and disabled for LAG interfaces.

14. Use the **Frame Size** field to specify the maximum Ethernet frame size the interface supports or is configured to use, including Ethernet header, CRC, and payload.

The range is 1518 to 9216. The default maximum frame size is 1518.

15. From the **Flow Control** menu, select to enable or disable IEEE 802.3 flow control.

The default is disabled. The switch does not send pause frames if the port buffers become full. Flow control helps to prevent data loss when the port cannot keep up with the number of frames being switched. When flow control is enabled, the switch can send

a pause frame to stop traffic on a 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 period of time 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. For LAG interfaces, flow control mode is displayed as a blank field because flow control is not applicable.

16. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information on the page.

Table 17. Port Configuration information

Field	Description
Port Type	For normal ports this field is blank. Otherwise, the possible values are as follows: <ul style="list-style-type: none"> • Mirrored. The port is a mirrored port on which all the traffic is copied to the probe port. • Probe. Use this port to monitor a mirrored port. • Trunk Member. The port is a member of a link aggregation trunk. Look at the LAG pages for more information.
Physical Status	Indicates the port speed and duplex mode.
Link Status	Indicates whether the link is up or down.
MAC Address	Displays the physical address of the specified interface.
PortList Bit Offset	Displays the bit offset value that corresponds to the port when the MIB object type PortList is used to manage in SNMP.
ifIndex	The ifIndex of the interface table entry associated with this port.

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. The LAG by default 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.

Static LAGs are supported. When a port is added to a LAG as a static member, it neither transmits nor receives LACPDUs. The switch supports eight LAGs.

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

LAG Configuration									
<input type="checkbox"/>	LAG Name	Description	LAG ID	Admin Mode	STP Mode	Link Trap	LAG Type	Active Ports	LAG state
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>		
<input type="checkbox"/>	LAG1		1	Enable	Enable	Disable	Static		Link Down
<input type="checkbox"/>	LAG2		2	Enable	Enable	Disable	Static		Link Down
<input type="checkbox"/>	LAG3		3	Enable	Enable	Disable	Static		Link Down
<input type="checkbox"/>	LAG4		4	Enable	Enable	Disable	Static		Link Down
<input type="checkbox"/>	LAG5		5	Enable	Enable	Disable	Static		Link Down
<input type="checkbox"/>	LAG6		6	Enable	Enable	Disable	Static		Link Down
<input type="checkbox"/>	LAG7		7	Enable	Enable	Disable	Static		Link Down
<input type="checkbox"/>	LAG8		8	Enable	Enable	Disable	Static		Link Down

6. 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. A valid name must be specified for you to create the LAG.

7. In the **Description** field, enter the description string to be attached to a 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 LACPDUs are dropped, but the links that form the LAG are not released. The default is Enable.

9. From the **STP Mode** menu, select the Spanning Tree Protocol (STP) administrative mode associated with the LAG. The possible values are as follows:
 - **Disable**. Spanning tree is disabled for this LAG.
 - **Enable**. Spanning tree is enabled for this LAG. Enable is the default.
10. 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.
11. 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**. Disables LACP on the selected LAG. The LAG is configured automatically.
12. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information on the page.

Table 18. LAG Configuration information

Field	Description
LAG ID	Identification of the LAG.
Active Ports	Indicates the ports that are actively participating in the port channel.
LAG State	Indicates whether the link is up or down.

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.

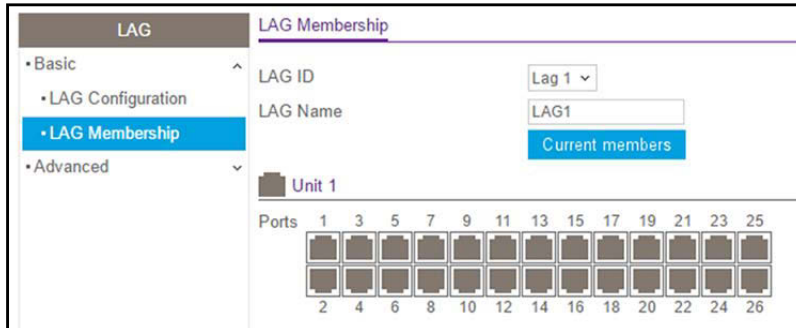
If you do not know the IP address of the switch, see [Change the Default IP Address of the Switch](#) on page 9.

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**.



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. A valid name must be specified for you to create the LAG.
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.
The updated configuration is sent to the switch. Configuration changes take effect immediately.

Set the LACP System Priority

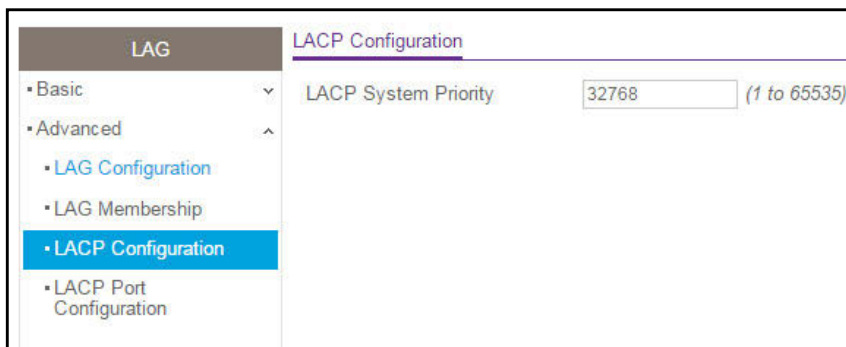
The LACP configuration page is used to set the LACP system priority.

➤ 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 [Change the Default IP Address of the Switch](#) on page 9.
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**.



LAG	LACP Configuration
• Basic	LACP System Priority <input type="text" value="32768"/> (1 to 65535)
• Advanced	
• LAG Configuration	
• LAG Membership	
• LACP Configuration	
• LACP Port Configuration	

6. In the **LACP System Priority** field, specify the device's link aggregation priority relative to the devices at the other ends of the links on which link aggregation is enabled.

A higher value indicates a lower priority. You can change the value of the parameter globally by specifying a priority from 1 to 65535. The default is 32768.

7. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

<input type="checkbox"/>	Interface	LACP Priority	Timeout
<input type="checkbox"/>	g1	128	Long
<input type="checkbox"/>	g2	128	Long
<input type="checkbox"/>	g3	128	Long
<input type="checkbox"/>	g4	128	Long
<input type="checkbox"/>	g5	128	Long
<input type="checkbox"/>	g6	128	Long
<input type="checkbox"/>	g7	128	Long
<input type="checkbox"/>	g8	128	Long

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 device's link aggregation priority relative to the devices at the other ends of the links on which link aggregation is enabled. A higher value indicates a lower priority. The range is 0 to 255. The default 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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 given 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 64 VLANs. VLAN 1 is created by default and is the default VLAN of which all ports are members.

Configure VLAN Settings

The internal VLAN is reserved by a port-based routing interface and invisible to the end user. Once these internal VLANs are allocated by the port-based routing interface, they cannot be assigned to a routing VLAN interface.

Add a Internal VLAN

➤ To add an internal 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 [Change the Default IP Address of the Switch](#) on page 9.

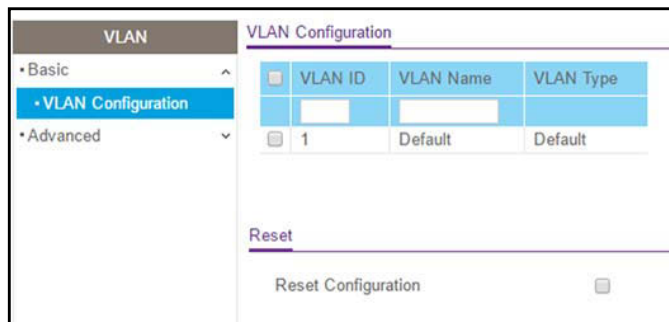
The login window opens.

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**.



6. In the **VLAN ID** field, specify the VLAN identifier for the new VLAN.

The range of the VLAN ID can be from 1 to 4093.

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. The default is blank. VLAN ID 1 always uses the name Default.

8. The **VLAN Type** field displays the type of the VLAN that you are configuring.

You cannot change the type of the default VLAN (VLAN ID = 1): it is always type Default. When you create a VLAN using this page, its type is always Static.

9. Click the **Add** button.

The VLAN is added to the switch.

10. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 1 to 4093.

Note: You cannot delete VLAN 1, which is created by default.

7. Click the **Delete** button.

The VLAN is removed.

Reset a VLAN to Its Default Settings

➤ To reset a VLAN to its 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 [Change the Default IP Address of the Switch](#) on page 9.

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. Select the **Reset Configuration** check box.

7. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The 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 VLANs, except for the default VLAN, 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 [Change the Default IP Address of the Switch](#) on page 9.

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 screenshot shows the 'VLAN Membership' configuration page. On the left is a navigation menu with 'VLAN Membership' selected. The main area has the following fields:

- VLAN ID: 1
- Group Operation: Untag All
- VLAN Name: Default
- VLAN Type: Default

Below these are two tables:

Unit 1	
Ports	1 3 5 7 9 11 13 15 17 19 21 23 25
	U U U U U U U U U U U U U U
	U U U U U U U U U U U U U U
	2 4 6 8 10 12 14 16 18 20 22 24 26

LAG	
LAG	1 3 5 7
	U U U U
	U U U U
	2 4 6 8

6. In the **VLAN ID** menu, select the VLAN ID.
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 that are members of the VLAN, tags are removed from all egress packets.
 - **Tag All.** For all ports that are members of the VLAN, all egress packets are tagged.
 - **Remove All.** All ports that were dynamically registered through GVRP 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 settings:
 - **T (Tagged).** Select the ports on which all frames transmitted for this VLAN are tagged. The ports that are selected are included in the VLAN.
 - **U (Untagged).** Select the ports on which all frames transmitted for this VLAN are untagged. The ports that are selected are included in the VLAN.
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 settings:
 - **T (Tagged).** Select the LAGs on which all frames transmitted for this VLAN are tagged. The LAGs that are selected are included in the VLAN.

- **U (Untagged).** Select the LAGs on which all frames transmitted for this VLAN are untagged. The LAGs that are selected are included in the VLAN.

10. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information on the page.

Table 19. Advanced VLAN membership

Field	Definition
VLAN Name	The name for the VLAN that you selected. It can be up to 32 alphanumeric characters long, including blanks. VLAN ID 1 always uses the name Default.
VLAN Type	The type of the VLAN you selected: <ul style="list-style-type: none"> • Default (VLAN ID = 1). Always present. • Static. A VLAN that you configured.

View 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

VLAN ID	VLAN Name	VLAN Type	Member Ports
1	Default	Default	g1 - g26, I1 - I8

The following table describes the nonconfigurable information on the page.

Table 20. VLAN status

Field	Definition
VLAN ID	The VLAN identifier (VID) of the VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	The name of the VLAN. VLAN ID 1 is always named Default.
VLAN Type	The VLAN type: <ul style="list-style-type: none"> • Default (VLAN ID = 1). Always present. • Static. A VLAN that you configured.
Member Ports	The ports 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:

- You must define a PVID for all ports.
- If no other value is specified, 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.

➤ 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Interface	PVID	VLAN Member	VLAN Tag	Acceptable Frame	Ingress Filtering	Current Ingress Filtering	Untagged VLANs	Tagged VLANs	Port Priority
<input type="checkbox"/> g1	1	1	None	Admit All	Disable	Disable	1	None	0
<input type="checkbox"/> g2	1	1	None	Admit All	Disable	Disable	1	None	0
<input type="checkbox"/> g3	1	1	None	Admit All	Disable	Disable	1	None	0
<input type="checkbox"/> g4	1	1	None	Admit All	Disable	Disable	1	None	0
<input type="checkbox"/> g5	1	1	None	Admit All	Disable	Disable	1	None	0
<input type="checkbox"/> g6	1	1	None	Admit All	Disable	Disable	1	None	0
<input type="checkbox"/> g7	1	1	None	Admit All	Disable	Disable	1	None	0
<input type="checkbox"/> g8	1	1	None	Admit All	Disable	Disable	1	None	0
<input type="checkbox"/> g9	1	1	None	Admit All	Disable	Disable	1	None	0
<input type="checkbox"/> g10	1	1	None	Admit All	Disable	Disable	1	None	0
<input type="checkbox"/> g11	1	1	None	Admit All	Disable	Disable	1	None	0

6. To display information for all physical ports and LAGs, click the **ALL** link.

7. Select interfaces by selecting the **Interface** check boxes next to the interfaces.

You can select multiple interfaces. To select all the interfaces, select the **Interface** 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 this port.

The default is 1.

9. In the **VLAN Member** field, specify the VLAN ID or list of VLANs of a member port.

VLAN IDs range from 1 to 4093. 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 1 to 4093. Use a hyphen (-) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted. To reset the VLAN tag configuration to the defaults, use the **None** keyword. Port tagging for the VLAN can be set only if the port is a member of this VLAN.

11. From the **Acceptable Frame** menu, specify the types of frames that can be received on this port.

The options are **VLAN only** and **Admit All**:

- **VLAN only.** Untagged frames or priority-tagged frames received on this port are discarded.
- **Admit All.** Untagged frames or priority-tagged frames received on this port are accepted and assigned the value of the port VLAN ID for this port. With either option, 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 this 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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable fields on the page.

Table 21. PVID Configuration information

Field	Description
Current Ingress Filtering	Displays whether ingress filtering is enabled for the interface.
Untagged VLANs	The number of untagged VLANs for the interface.
Tagged VLANs	The number of tagged VLANs for the interface.

Configure a Voice VLAN

You can configure the parameters 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Interface	Interface Mode	Value	CoS Override Mode	Operational State	Authentication Mode	DSCP Value
<input type="checkbox"/> g1	Disable	0	Disable	Disable	Enable	0
<input type="checkbox"/> g2	Disable	0	Disable	Disable	Enable	0
<input type="checkbox"/> g3	Disable	0	Disable	Disable	Enable	0
<input type="checkbox"/> g4	Disable	0	Disable	Disable	Enable	0
<input type="checkbox"/> g5	Disable	0	Disable	Disable	Enable	0
<input type="checkbox"/> g6	Disable	0	Disable	Disable	Enable	0
<input type="checkbox"/> g7	Disable	0	Disable	Disable	Enable	0
<input type="checkbox"/> g8	Disable	0	Disable	Disable	Enable	0
<input type="checkbox"/> g9	Disable	0	Disable	Disable	Enable	0
<input type="checkbox"/> g10	Disable	0	Disable	Disable	Enable	0
<input type="checkbox"/> g11	Disable	0	Disable	Disable	Enable	0
<input type="checkbox"/> g12	Disable	0	Disable	Disable	Enable	0

6. Select the Admin Mode **Disable** or **Enable** radio button.

This 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.
- **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.
- **Dot1p**. Configure voice VLAN 802.1p priority tagging for voice traffic. When this is selected, enter the dot1p value in the **Value** field.
- **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 when VLAN ID or dot1p is selected as the interface mode.

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 valid range is 0 to 63. The default is 0.

The Operational State field displays the operational status of the voice VLAN on the given interface.

13. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 helps provide a classification mechanism for voice packets so that they can be prioritized above data packets in order to provide better Quality of Service (QoS). With the Auto-VoIP feature, voice prioritization is provided based on call-control protocols (SIP, SCCP, H.323) or OUI bits.

Configure Protocol-Based Port Settings

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:

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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Protocol-based > Port Settings**.

The screenshot shows the configuration interface for Auto-VoIP. On the left, a navigation menu includes 'Auto-VoIP', 'Protocol-based', 'Port Settings' (selected), 'OUI-based', and 'Auto-VoIP Status'. The main area is divided into two sections: 'Protocol Based Global Settings' and 'Protocol Based Port Settings'. In the global settings, 'Prioritization Type' is set to 'Traffic Class' and 'Class Value' is set to '7'. The port settings section has a 'Go To Interface' field and a 'Go' button. Below is a table with columns for 'Interface', 'Auto-VoIP Mode', and 'Operational Status'.

Interface	Auto-VoIP Mode	Operational Status
g1	Disable	Down
g2	Disable	Down
g3	Disable	Down
g4	Disable	Down
g5	Disable	Down
g6	Disable	Down
g7	Disable	Down
g8	Disable	Down
g9	Disable	Down

6. From the **Prioritization Type** menu, select **Traffic Class** or **Remark**.

This specifies the type of prioritization.

7. From the **Class Value** menu, specify the CoS tag value to be reassigned for packets received on the voice VLAN when Remark CoS is enabled.

8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

OUI Based Properties	
Auto-VoIP VLAN ID	<input type="text" value="0"/> (1 to 4093)
OUI-based priority	<input type="text" value="7"/> ▾

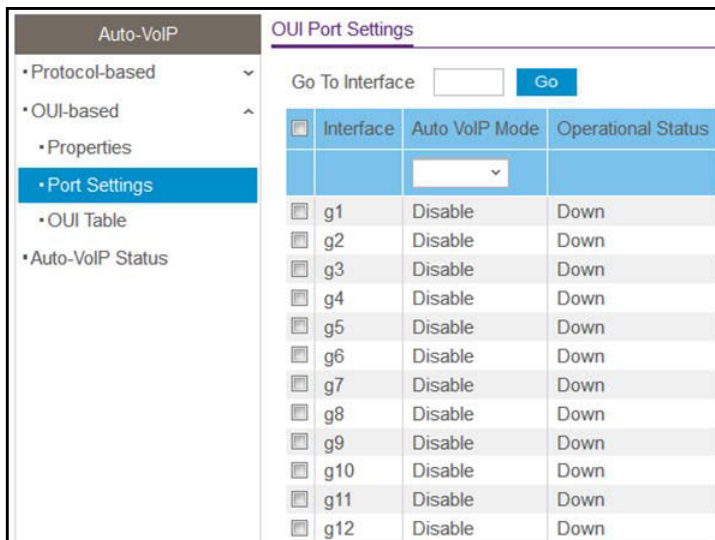
6. In the **Auto-VoIP VLAN ID** field, enter the VoIP VLAN ID of the switch.
No default VLAN exists for Auto-VoIP, you must create a VLAN for Auto-VoIP.
7. From the **OUI-based priority** menu, select the OUI-based priority of the switch.
The default is 7.
8. Click the **Apply** button.
The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure OUI-Based Port Settings

The port settings page allows you to 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 [Change the Default IP Address of the Switch](#) on page 9.
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**.



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 VoIP Mode** menu, select **Disable** or **Enable**.

Auto-VoIP is disabled by default.

The **Operational Status** field displays the current operational status of each interface.

8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

<input type="checkbox"/>	Telephony OUI(s)	Description
<input type="checkbox"/>	00:01:E3	SIEMENS
<input type="checkbox"/>	00:03:6B	CISCO1
<input type="checkbox"/>	00:12:43	CISCO2
<input type="checkbox"/>	00:0F:E2	H3C
<input type="checkbox"/>	00:60:B9	NITSUKO
<input type="checkbox"/>	00:D0:1E	PINTEL
<input type="checkbox"/>	00:E0:75	VERILINK
<input type="checkbox"/>	00:E0:BB	3COM
<input type="checkbox"/>	00:04:0D	AVAYA1
<input type="checkbox"/>	00:1B:4F	AVAYA2
<input type="checkbox"/>	00:04:13	SNOM

6. In the **Telephony OUI(s)** field, specify the VoIP OUI prefix to be added in the format AA:BB:CC.

Up to 52 OUIs can be configured.

7. In the **Description** field, enter the description for the OUI.

The maximum length of description is 32 characters. The following OUIs are present in the configuration by default:

- 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

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 [Change the Default IP Address of the Switch](#) on page 9.

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Auto-VoIP	Auto-VoIP Status	
• Protocol-based	Auto-VoIP VLAN ID	0
• OUI-based	Maximum Number of Voice Channels Supported	20
• Auto-VoIP Status	Number of Voice Channels Detected	0

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

The following table describes the nonconfigurable Auto-VoIP status information on the page.

Table 22. Auto-VoIP status information

Field	Description
Auto-VoIP VLAN ID	The Auto-VoIP VLAN ID.
Maximum Number of Voice Channels Supported	The maximum number of voice channels supported.
Number of Voice Channels Detected	The number of VoIP channels prioritized successfully.

Configure Spanning Tree Protocol

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

Classic STP provides a single path between end stations, avoiding and eliminating loops. For information on configuring Common STP, see [Configure CST Port Settings](#) on page 121.

Multiple Spanning Tree Protocol (MSTP) supports multiple instances of spanning tree to efficiently channel VLAN traffic over different interfaces. Each instance of the spanning tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree (RSTP), with slight modifications in the working but not the end effect (chief among the effects is the rapid transitioning of the port to 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 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 STP Settings

The STP Configuration page contains fields for enabling STP on the switch.

➤ **To configure STP 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

The following figure does not show the STP Status section on the page.

STP	
Basic	Spanning Tree State <input type="radio"/> Disable <input checked="" type="radio"/> Enable
STP Configuration	STP Operation Mode <input type="radio"/> STP <input type="radio"/> RSTP <input checked="" type="radio"/> MSTP
Advanced	Configuration Name <input type="text" value="9c-3d-cf-fb-a5-04"/>
	Configuration Revision Level <input type="text" value="0"/> (0 to 65535)
	Configuration Digest Key <input type="text" value="0xac36177f50283cd4b83821d8ab26de62"/>
	BPDU Flooding <input checked="" type="radio"/> Disable <input type="radio"/> Enable

6. Configure the following options:

- **Spanning Tree State.** Enable or disable the spanning tree operation on the switch.
- **STP Operation Mode.** Specify the STP version for the switch. The options are **STP**, **RSTP**, and **MSTP**.
- **Configuration Name.** Specify an identifier used to identify the configuration currently being used. It can be up to 32 alphanumeric characters.
- **Configuration Revision Level.** Specify an identifier used to identify the configuration currently being used. The values allowed are between 0 and 65535. The default is 0.
- **BPDU Flooding.** Enable or disable the BPDU flood. This specifies whether spanning tree BPDUs are forwarded or not while spanning tree is disabled on the switch.

The Configuration Digest Key field shows the identifier for the configuration that is in use.

7. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable STP Status fields displayed on the page.

Table 23. STP configuration status

Field	Description
Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	The time in day-hour-minute-second format since the topology of the CST last changed.
Topology Change Count	The number of times that the topology changed for the CST.
Topology Change	The value of the topology change parameter for the switch indicating whether a topology change is in progress on any port assigned to the CST. Possible values are True and False.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Path cost to the designated root for the CST.

Table 23. STP configuration status (continued)

Field	Description
Root Port	Port to access the designated root for the CST.
Max Age (secs)	The maximum age timer controls the maximum length of time in seconds that passes before a bridge port saves its configuration BPDU information.
Forward Delay (secs)	The derived value of the Root Port Bridge Forward Delay parameter.
Hold Time (secs)	Minimum time in seconds between the transmission of configuration BPDUs.
CST Regional Root	Priority and base MAC address of the CST regional root.
CST Path Cost	Path cost to the CST tree regional root.

Configure CST Settings

You can configure Common Spanning Tree (CST) and Internal Spanning Tree on the switch.

➤ To configure 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

STP		CST Configuration	
• Basic	▼	Bridge Priority	<input type="text" value="32768"/> (0 to 61440)
• Advanced	▲	Bridge Max Age (secs)	<input type="text" value="20"/> (6 to 40)
• STP Configuration		Bridge Hello Time (secs)	<input type="text" value="2"/>
• CST Configuration		Bridge Forward Delay (secs)	<input type="text" value="15"/> (4 to 30)
• CST Port Configuration			
• CST Port Status			
• RSTP			
• MST Configuration			
• MST Port Configuration			
• STP Statistics			

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 valid range is 0–61440. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if you set the priority to any value between 0 and 4095, the switch automatically sets the value to 0. The default 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 valid range is 6–40, and the value must be less than or equal to $(2 * \text{Bridge Forward Delay}) - 1$ and greater than or equal to $2 * (\text{Bridge Hello Time} + 1)$. The default 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 $(\text{Bridge Max Age} / 2) - 1$. 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 $(\text{Bridge Max Age} / 2) + 1$. The time range is from 4 seconds to 30 seconds. The default is 15 seconds.

7. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure CST Port Settings

You can configure 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 extremely rare.

➤ To configure 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Interface	STP Status	Fast Link	Port State	Path Cost	Priority	Port ID	Hello Timer
<input type="checkbox"/> g1	Disable	Enable	Disabled	0	128	32769	2
<input type="checkbox"/> g2	Disable	Enable	Disabled	0	128	32770	2
<input type="checkbox"/> g3	Disable	Enable	Disabled	0	128	32771	2
<input type="checkbox"/> g4	Disable	Enable	Disabled	0	128	32772	2
<input type="checkbox"/> g5	Disable	Enable	Disabled	0	128	32773	2
<input type="checkbox"/> g6	Disable	Enable	Disabled	0	128	32774	2
<input type="checkbox"/> g7	Disable	Enable	Disabled	0	128	32775	2
<input type="checkbox"/> g8	Disable	Enable	Disabled	0	128	32776	2
<input type="checkbox"/> g9	Disable	Enable	Disabled	0	128	32777	2
<input type="checkbox"/> g10	Disable	Enable	Disabled	0	128	32778	2

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.

- From the **STP Status** menu, select the option to enable or disable the spanning tree administrative mode that is associated with the port or port channel.

The possible values are **Enable** and **Disable**. The default is Enable.

- From the **Fast Link** menu, select whether the specified port is an edge port within the CST.

The possible values are **Enable** and **Disable**. The default is Enable.

- 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 of 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 a received STP packet.

- 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 $(2*16 - 1)$, it is set to 16, and so on. The range is 0 to 240. The default is 128.

- Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

- To refresh the page with the latest information about the switch, click the **Update** button.

The following table describes the nonconfigurable information on the page.

Table 24. CST port configuration

Field	Description
Port State	The forwarding state of this port. The default is Disabled.
Port ID	The port identifier for the specified port within the CST. It is made up from the port priority and the interface number of the port.
Hello Timer	The value of the parameter for the CST. The default is 2 seconds.

View CST Port Status

You can display Common Spanning Tree (CST) and Internal Spanning Tree on a specific port on the switch.

➤ To view the CST port status:

- 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.

- Launch a web browser.

- 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 [Change the Default IP Address of the Switch](#) on page 9.

The login window opens.

- Enter the switch's password in the **Password** field.

The default password is **password**.

The System Information page displays.

- Select **Switching > STP > Advanced > CST Port Status**.

Interface	Port Role	Designated Root	Designated Cost	Designated Bridge	Designated Port	Topology Change Acknowledge	Edge Port	Point-to-Point MAC	Port Forwarding State
g1	Disabled	80 00 08 02 9e 8d 1f 88	0	80 00 08 02 9e 8d 1f 88	0	False	False	False	Disabled
g2	Designated	80 00 08 02 9e 8d 1f 88	0	80 00 08 02 9e 8d 1f 88	32770	False	False	True	Forwarding
g3	Disabled	80 00 08 02 9e 8d 1f 88	0	80 00 08 02 9e 8d 1f 88	0	False	False	False	Disabled
g4	Disabled	80 00 08 02 9e 8d 1f 88	0	80 00 08 02 9e 8d 1f 88	0	False	False	False	Disabled
g5	Disabled	80 00 08 02 9e 8d 1f 88	0	80 00 08 02 9e 8d 1f 88	0	False	False	False	Disabled
g6	Disabled	80 00 08 02 9e 8d 1f 88	0	80 00 08 02 9e 8d 1f 88	0	False	False	False	Disabled
g7	Disabled	80 00 08 02 9e 8d 1f 88	0	80 00 08 02 9e 8d 1f 88	0	False	False	False	Disabled
g8	Disabled	80 00 08 02 9e 8d 1f 88	0	80 00 08 02 9e 8d 1f 88	0	False	False	False	Disabled
g9	Disabled	80 00 08 02 9e 8d 1f 88	0	80 00 08 02 9e 8d 1f 88	0	False	False	False	Disabled
g10	Disabled	80 00 08 02 9e 8d 1f 88	0	80 00 08 02 9e 8d 1f 88	0	False	False	False	Disabled
g11	Disabled	80 00 08 02 9e 8d 1f 88	0	80 00 08 02 9e 8d 1f 88	0	False	False	False	Disabled
g12	Disabled	80 00 08 02 9e 8d 1f 88	0	80 00 08 02 9e 8d 1f 88	0	False	False	False	Disabled

- To refresh the page with the latest information about the switch, click the **Update** button.

The following table describes the CST port status information on the page.

Table 25. CST port status

Field	Description
Interface	Identify the physical or port channel interfaces associated with VLANs associated with the CST.
Port Role	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 Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.
Designated Root	Root bridge for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	Path cost offered to the LAN by the designated port.
Designated Bridge	Bridge identifier of the bridge with the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	Port identifier on the designated bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.
Topology Change Acknowledge	Identifies whether the topology change acknowledgement flag is set for the next BPDU to be transmitted for this port. It is either True or False.
Edge port	Indicates whether the port is enabled as an edge port. It is either Enabled or Disabled.
Point-to-point MAC	Derived value of the point-to-point status.

Table 25. CST port status (continued)

Field	Description
CST Regional Root	Bridge identifier of the CST regional root. It is made up using the bridge priority and the base MAC address of the bridge.
CST Path Cost	Path cost to the CST regional root.
Port Forwarding State	The forwarding state of this port.

View Rapid STP Information

You can view information about the status of the Rapid Spanning Tree (RSTP) port.

➤ **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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

The Rapid STP page displays.

The following table describes the Rapid STP status information on the page.

Table 26. Rapid STP status information

Field	Description
Interface	The physical or port channel interfaces associated with VLANs associated with the CST.
Role	Each MST bridge port that is enabled is assigned a port role for each spanning tree. The port role is one of the following: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.
Mode	Specifies the spanning tree operation mode. Different modes are STP, RSTP, and MSTP.
Fast Link	Indicates whether the port is enabled as an edge port.
Status	The forwarding state of this port.

Manage MST Settings

You can configure 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

MST ID	Priority	Vlan Id	Bridge Identifier	Last TCN	Topology Change Count	Topology Change	Designated Root	Root Path Cost	Root Port
0	32768	1,4089	80:00:00:0D:70:16:58:12	2 day 14 hr 29 min 54 sec	0	False	80:00:00:0D:70:16:58:12	0	00:00

6. Configure the MST values:

- **MST ID.** Specify the ID of the MST to create. The valid values for this are 1 to 64. This is visible only when the select option of the MST ID select box is selected. The switch supports up to four instances.
- **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 is 32768. The valid range is 0–61440.
- **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.

The following table describes the nonconfigurable information on the page.

Table 27. MST configuration

Field	Description
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Last TCN	The time in day:hour:minute:second format since the topology of the selected MST instance last changed.
Topology Change Count	Number of times that the topology changed for the selected MST instance.
Topology Change	The value of the topology change parameter 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.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge
Root Path Cost	Path cost to the designated root for this MST instance.
Root Port	Port to access the designated root for this MST instance.

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 [Change the Default IP Address of the Switch](#) on page 9.

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.
7. Update the values.
8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 the MST Port Settings

You can configure and display 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 MST 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 [Change the Default IP Address of the Switch](#) on page 9.

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 Status page displays.

Note: If no MST instances were configured on the switch, the page displays a "No MSTs Available" message.

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. 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 automatically set to the next lowest priority that is a multiple of 16. For example, if you set a value between 0 and 15, the priority is set to 0. If you specify a number between 16 and 31, the priority is set to 16. Specify a value in the range of 0–240.
- **Port Path Cost.** Set the path cost to a new value for the specified port in the selected MST instance. Specify a value in the range of 0–200000000.

8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information on the page.

Table 28. MST port status information

Field	Description
Auto-calculated Port Path Cost	Displays 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.
Port ID	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.
Port Up Time Since Counters Last Cleared	Time since the counters were last cleared, displayed in days, hours, minutes, and seconds.
Port Mode	Spanning Tree Protocol administrative mode associated with the port or port channel. Possible values are Enable or Disable.
Port Forwarding State	Indicates the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are as follows: <ul style="list-style-type: none"> • Disabled. STP is currently disabled on the port. The port forwards traffic while learning MAC addresses. • Blocking. The port is currently blocked and cannot be used to forward traffic or learn MAC addresses. • Listening. The port is currently in the listening mode. The port cannot forward traffic nor can it learn MAC addresses. • Learning. The port is currently in the learning mode. The port cannot forward traffic. However, it can learn new MAC addresses. • Forwarding. The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses
Port Role	Each MST bridge port that is enabled is assigned a port role for each spanning tree. The port role is one of the following: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.
Designated Root	Root bridge for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	Displays cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
Designated Bridge	Bridge identifier of the bridge with the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	Port identifier on the designated bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.

View STP Statistics

You can view information about the number and type of bridge protocol data units (BPDUs) transmitted and received on each port.

➤ **To view 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Interface	STP BPDUs Received	STP BPDUs Transmitted	RSTP BPDUs Received	RSTP BPDUs Transmitted	MSTP BPDUs Received	MSTP BPDUs Transmitted
g1	0	0	0	0	0	0
g2	0	0	0	18833	0	0
g3	0	0	0	0	0	0
g4	0	0	0	0	0	0
g5	0	0	0	0	0	0
g6	0	0	0	0	0	0
g7	0	0	0	0	0	0
g8	0	0	0	0	0	0
g9	0	0	0	0	0	0
g10	0	0	0	0	0	0
g11	0	0	0	0	0	0
g12	0	0	0	0	0	0

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

The following table describes the nonconfigurable information on the page.

Table 29. STP Statistics

Field	Description
Interface	Selects one of the physical or port channel interfaces of the switch.
STP BPDUs Received	Number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	Number of STP BPDUs transmitted from the selected port.
RSTP BPDUs Received	Number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	Number of RSTP BPDUs transmitted from the selected port.

Table 29. STP Statistics (continued)

Field	Description
MSTP BPDUs Received	Number of MSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	Number of MSTP BPDUs transmitted from the selected port.

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. Host groups for IPv6 multicast are identified by the prefix ff00::/8.

View the MFDB Table

The Multicast Forwarding Database 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 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 [Change the Default IP Address of the Switch](#) on page 9.

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 01:00:5e:45:67:89.

7. Click the **Go** button.

If the address exists, the entry is displayed. An exact match is required.

The following describes the nonconfigurable information on the page.

Table 30. MFDB table information

Field	Description
MAC Address	The multicast MAC address for which you requested data.
VLAN ID	The VLAN ID to which the multicast MAC address is related.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Component	This is the component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP snooping, GMRP, Static Filtering and MLD snooping.
Description	The text description of this multicast table entry. Possible values are Management Configured, Network Configured, and Network Assisted.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:) for the selected address.
Forwarding Interfaces	The resultant forwarding list is derived from combining all the forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

MFDB Statistics	
Max MFDB Table Entries	128
Most MFDB Entries Since Last Reset	0
Current Entries	0

The following table describes the nonconfigurable information on the page.

Table 31. MFDB Statistics information

Field	Description
Max MFDB Table Entries	The maximum number of entries that the Multicast Forwarding Database table can hold.
Most MFDB Entries Since Last Reset	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.
Current Entries	The current number of entries in the Multicast Forwarding Database table.

IGMP Snooping Overview

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

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

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

Configure IGMP Snooping

You can configure the parameters 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 [Change the Default IP Address of the Switch](#) on page 9.

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 Configuration**.

The following figure does not display all information on the page.

IGMP Snooping Configuration	
IGMP Snooping Status	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Validate IGMP IP header	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
IGMP Statistics	
Multicast Control Frame Count	0
Interfaces Enabled for IGMP Snooping	
VLAN Ids Enabled for IGMP Snooping	
VLAN Ids Enabled for IGMP Snooping Querier	

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 is Disable.

8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

9. To refresh the page with the latest information about the switch, click the **Update** button.

The following table describes the nonconfigurable information on the page.

Table 32. IGMP Snooping Configuration information

Field	Description
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
Interfaces Enabled for IGMP Snooping	A list of all the interfaces currently enabled for IGMP snooping.
VLAN IDs Enabled For IGMP Snooping	Displays VLAN IDs enabled for IGMP snooping.
VLAN IDs Enabled For IGMP Snooping Querier	Displays VLAN IDs enabled for IGMP snooping querier.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 Interface Configuration**.

Multicast		IGMP Snooping Interface Configuration						
* MFDB	▼	1 LAG All						
* IGMP Snooping	▲	Go To Interface <input type="text"/> <input type="button" value="Go"/>						
* IGMP Snooping Configuration		<input type="checkbox"/>	Interface	Admin Mode	Host Timeout	Max Response Time	MRouter Timeout	Fast Leave Mode
* IGMP Snooping Interface Configuration		<input type="checkbox"/>		▼				▼
* IGMP Snooping Table		<input type="checkbox"/>	g1	Disable	260	10	0	Disable
* IGMP Snooping VLAN Configuration		<input type="checkbox"/>	g2	Disable	260	10	0	Disable
* IGMP Snooping Querier	▼	<input type="checkbox"/>	g3	Disable	260	10	0	Disable
* Static Multicast Address	▼	<input type="checkbox"/>	g4	Disable	260	10	0	Disable
		<input type="checkbox"/>	g5	Disable	260	10	0	Disable
		<input type="checkbox"/>	g6	Disable	260	10	0	Disable
		<input type="checkbox"/>	g7	Disable	260	10	0	Disable
		<input type="checkbox"/>	g8	Disable	260	10	0	Disable

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 **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.
8. 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 2 and 3600 seconds. The default is 260 seconds.
9. 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 between 1 and 25 seconds. The default is 10 seconds. The configured value must be less than the value in the **Host Timeout** field.
10. 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.
11. From the **Fast Leave Mode** menu, select whether fast leave mode is enabled.
The options are **Enable** and **Disable**. The default is Disable.
12. Click the **Apply** button.
The updated configuration is sent to the switch. Configuration changes take effect immediately.

View the IGMP Snooping Table

You can view all of the entries in the Multicast Forwarding Database that were created for IGMP snooping.

➤ **To view the entries in 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 [Change the Default IP Address of the Switch](#) on page 9.

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 for which you want to view the entry in the MFDB table.

Enter six two-digit hexadecimal numbers separated by colons, for example 01:00:5e:45:67:89.

7. Click the **Go** button.

If the address exists, the entry is displayed. An exact match is required.

The following table describes the nonconfigurable information on the page.

Table 33. IGMP Snooping Table information

Field	Description
MAC Address	A 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.
VLAN ID	A VLAN ID for which the switch holds forwarding and filtering information.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Table 33. IGMP Snooping Table information (continued)

Field	Description
Description	The text description of this multicast table entry. Possible values are Management Configured, Network Configured, and Network Assisted.
Interface	The list of interfaces that are designated for forwarding (Fwd) and filtering (Flt) for the associated address.

Configure IGMP Snooping for VLANs

➤ 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

IGMP Snooping VLAN Configuration								
<input type="checkbox"/>	VLAN ID	Admin Mode	Fast Leave Mode	Host Timeout	Maximum Response Time	MRouter Timeout	Query Mode	Query Interval (1 to 1800 secs)
<input type="checkbox"/>								
<input type="checkbox"/>	1	Disable	Disable	260	10	0	Disable	60
<input type="checkbox"/>	3	Disable	Disable	260	10	0	Disable	60
<input type="checkbox"/>	5	Disable	Disable	260	10	0	Disable	60
<input type="checkbox"/>	6	Disable	Disable	260	10	0	Disable	60
<input type="checkbox"/>	10	Disable	Disable	260	10	0	Disable	60
<input type="checkbox"/>	22	Disable	Disable	260	10	0	Disable	60
<input type="checkbox"/>	4089	Disable	Disable	260	10	0	Disable	60

When you create a VLAN, the VLAN is automatically added to the IGMP Snooping VLAN Configuration page.

6. Configure the IGMP snooping values:
 - **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.** Specify the time that the switch must wait for a report for a particular group for the specified VLAN ID. The valid range is the value in the **Maximum Response Time** plus 1 to 3600 seconds. The default is 260 seconds.
 - **Maximum Response Time.** Specify the time that the switch must wait after sending a query for the specified VLAN ID if the switch does not receive a report for a particular group for that VLAN ID. Enter a value between 1 and 25 seconds. The default is 10 seconds. The configured value must be less than the value in the **Host Timeout** field.
 - **MRouter Timeout.** Set the value for multicast router expiry time of IGMP snooping for the specified VLAN ID. The valid range is 0 to 3600 seconds. The default is 0 seconds.
 - **Querier Mode.** Enable or disable the IGMP Querier Mode for the specified VLAN ID. The default is Disable.
 - **Query Interval.** Set the IGMP query interval for the specified VLAN ID. The valid range is 1 to 1800 seconds. The default is 60 seconds.
7. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

IGMP Snooping Querier Overview

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

You can configure the parameters for IGMP snooping querier. Only a user with read/write access privileges can change the data on this page.

➤ To configure IGMP snooping querier 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Querier Configuration	
Querier Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Snooping Querier Address	<input type="text" value="0.0.0.0"/>
IGMP Version	<input type="text" value="2"/> (1 to 2)
Query Interval(secs)	<input type="text" value="60"/> (1 to 1800)
Querier Expiry Interval(secs)	<input type="text" value="125"/> (60 to 300)

6. Configure the following settings:
 - **Querier Admin Mode.** Enable or disable IGMP snooping for the switch. The default is Disable.

- **Snooping Querier IP Address.** Enter the snooping querier IP address to be used as the source address in periodic IGMP queries. This address is used when no address is configured on the VLAN on which a query is being sent.
- **IGMP Version.** Specify the IGMP protocol version used in periodic IGMP queries. The range is 1 to 2. The default is 2.
- **Query Interval(secs).** Specify the time interval in seconds between periodic queries sent by the snooping querier. The query interval must be a value in the range of 1 and 1800. The default is 60.
- **Querier Expiry Interval(secs).** Specify the time interval in seconds after which the last querier information is removed. The querier expiry Interval must be a value in the range of 60 and 300. The default is 125.

7. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure IGMP Snooping Querier for VLANs

You can configure IGMP queriers for use with VLANs on the network.

➤ **To create a new VLAN ID for 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

7. Configure the following settings:
 - **VLAN ID.** The VLAN ID for which the IGMP snooping querier is to be enabled.
 - **Querier Election Participate Mode.** Enable or disable querier this 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 sent on the specified VLAN.
8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.
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**.

Querier VLAN Status					
VLAN ID	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time(sec)

The following table describes the nonconfigurable information on the page.

Table 34. Querier VLAN Status information

Field	Description
VLAN ID	The VLAN ID on which IGMP snooping querier is administratively enabled and the VLAN exists in the VLAN database.
Operational State	The operational state of the IGMP snooping querier on a VLAN. It can be in any of the following states: <ul style="list-style-type: none"> • Querier. 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. • Non-Querier. 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. • Disabled. 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.
Operational Version	The operational IGMP protocol version of the querier.
Last Querier Address	The IP address of the last querier from which a query was snooped on the VLAN.
Last Querier Version	The IGMP protocol version of the last querier from which a query was snooped on the VLAN.
Operational Max Response Time	Displays maximum response time to be used in the queries that are sent by the snooping querier.

Configure a Static Multicast Group

You can configure up to 32 static multicast groups. You create a static multicast group by adding a multicast MAC address to a VLAN. The multicast MAC address becomes the group identifier.

➤ To configure a static multicast 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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Static Multicast Address > Multicast Group Configuration**.

Multicast Group Configuration				
	VLAN ID	VLAN Name	Multicast Address	Type
	▼			
<input type="checkbox"/>	1	Default	01:00:5e:01:02:03	Static
<input type="checkbox"/>	1	Default	01:00:5e:33:31:05	Static
<input type="checkbox"/>	1	Default	01:00:5e:51:01:02	Static

6. From the **VLAN ID** menu, select the VLAN ID.
7. In the **Multicast Address** field, enter the multicast MAC address that must become the group identifier.
8. Click the **Add** button.

The multicast group is added.

The following table describes the nonconfigurable information on the page.

Table 35. Multicast Group Configuration information

Field	Definition
VLAN Name	The VLAN name, if any, that is associated with the VLAN ID.
Type	The type of multicast group, which is determined by the way in which members are added to the group: <ul style="list-style-type: none"> • Dynamic. Members are added dynamically to the multicast group. By default, all groups are dynamic groups. • Static. If you add static members to the multicast group (see Configure Multicast Group Membership on page 145), the group becomes a static group.

Remove a Static Multicast Group

You can remove a static multicast group that you no longer need. Because the multicast MAC address is the multicast group identifier. You remove a static multicast group by removing the static multicast address from the VLAN to which it is assigned.

➤ To remove one or more static multicast groups:

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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Static Multicast Address > Multicast Group Configuration**.

The Multicast Group Configuration page displays.

6. Select the check boxes for the statically added multicast addresses that you want to remove.

7. Click the **Delete** button.

The multicast groups are removed.

Configure Multicast Group Membership

By default, an interface is excluded from multicast groups but could be dynamically added to any multicast group. You can manually add interfaces to a group (which changes the type of the group from dynamic to static) and you can lock interfaces so that they cannot be added dynamically to a group.

➤ To configure multicast 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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Static Multicast Address > Multicast Group Membership**.

6. From the **VLAN ID** menu, select the VLAN ID for the VLAN in which the multicast group is located.
If a name is associated with the VLAN, the name displays in the VLAN Name field.
7. From the **Multicast Address** menu, select the MAC address that identifies the multicast group.
8. Select which type of interfaces display onscreen:
 - To display physical ports only, click the **1** link.
 - To display LAGs only, click the **LAG** link.
 - To display both physical ports and LAGs, click the **All** link.
9. 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.
10. From the **Interface Status** menu, select one of the following options:
 - **Static**. The interface becomes a static member of the multicast group on the selected VLAN.
 - **Forbidden**. The interface is forbidden from joining the multicast group on the selected VLAN.
 - **Excluded**. The interface is not a static member of the multicast group but could become a dynamic member of a multicast group on the selected VLAN. This is the default state.

Note: If an interface was added dynamically to the multicast group as a result of IGMP or MLD snooping, the status of the interface is Dynamic. You cannot select this status manually.

11. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure the Multicast Forward All Option

After IGMP snooping is enabled, multicast packets are forwarded only to the members of multicast groups. However, you can enable the Multicast Forward All option for an interface so that the interface receives and forwards all multicast traffic on the VLAN.

➤ **To enable the Multicast Forward All option 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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Static Multicast Address > Multicast Forward All**.

The screenshot shows the 'Multicast Forward All' configuration page. It includes a 'VLAN ID' dropdown menu and a 'VLAN Name' field. Below this is a table with columns 'Interface' and 'Interface Status'. The table has one row with a checkbox, a dropdown menu, and a 'Go' button. At the bottom, there is a 'LAG All' link and another 'Go To Interface' field with a 'Go' button.

6. From the **VLAN ID** menu, select the VLAN ID for the VLAN in which the multicast group is located.

If a name is associated with the VLAN, the name displays in the VLAN Name field.

7. Select which type of interfaces display onscreen:

- To display physical ports only, click the **1** link.

- To display LAGs only, click the **LAG** link.
 - To display both physical ports and LAGs, click the **All** link.
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 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.
 9. From the **Interface Status** menu, select one of the following options:
 - **Static**. The interface receives all multicast traffic on the VLAN and forwards the traffic.
 - **Forbidden**. The interface cannot receive any multicast traffic on the VLAN, even if the IGMP or MLD snooping process designated the interface as a member of a multicast group.
 - **Excluded**. The Multicast Forward All option is not enabled on the interface, that is, the interface does not forward all multicast traffic on the VLAN. This is the default state.
 10. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

View and Configure 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 is used by the transparent bridging function in determining how to propagate a received frame.

Configure the MAC Address Table

➤ To configure 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 [Change the Default IP Address of the Switch](#) on page 9.

The login window opens.

- Enter the switch's password in the **Password** field.

The default password is **password**.

The System Information page displays.

- Select **Switching > Address Table > Basic > Address Table**.

VLAN ID	MAC Address	Interface	Status
1	00:00:00:00:00:10	g11	Learned
1	00:04:F2:40:A7:92	g23	Learned
1	00:05:1B:A2:F2:E1	g11	Learned
1	00:05:1B:A2:FD:6A	g11	Learned
1	00:05:9A:8E:3A:8A	g11	Learned
1	00:07:84:7F:47:FC	g11	Learned
1	00:08:03:08:09:15	g11	Learned
1	00:0B:AB:5C:13:30	g11	Learned

- 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.

The following table describes the nonconfigurable information on the page.

Table 36. MAC Address Table information

Field	Description
Total MAC Address	The number of total MAC addresses learned or configured.
MAC Address	A 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.
VLAN ID	The VLAN ID associated with the MAC address.

Table 36. MAC Address Table information (continued)

Field	Description
Interface	The interface upon which this address was learned.
Status	The status of this entry. The meanings of the values are as follows: <ul style="list-style-type: none"> • Static. The value of the corresponding instance was added by the system or a user and cannot be relearned. • Learned. The value of the corresponding instance was learned, and is being used. • Management. The value of the corresponding instance is also the value of an existing instance of dot1dStaticAddress.

Set the Dynamic Address Aging Interval

You can set the address aging interval for the specified 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 [Change the Default IP Address of the Switch](#) on page 9.

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

Address Aging Timeout (seconds) (10 to 1000000)

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure a Static MAC Address

➤ To configure a static MAC address:

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Address Table		Port List	
• Basic	▼	Interface	g1 ▼
• Advanced	▲	Static MAC Address	
• Dynamic Address		<input type="checkbox"/> Static MAC Address	VLAN ID
• Address Table		<input type="text"/>	▼
• Static MAC Address			

6. From the **Interface** menu, select the interface.
7. In the **Static MAC Address** field, enter the MAC address.
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.

4 Configure Quality of Service

4

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 get 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.

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.

This chapter contains the following sections:

- *Manage Class of Service*
- *Manage Differentiated Services*

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.

Eight queues per port are supported.

CoS Configuration Overview

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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Basic > CoS Configuration**.

6. Either configure the same CoS trust mode settings for all CoS-configurable interfaces or configure CoS settings per interface:

- 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**. The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of seven internal hardware priority queues. 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.
- To configure CoS settings per interface, do the following:
 - a. Select the **Interface** radio button.
 - b. From the **Interface Trust Mode** menu, select one of the following trust mode options:
 - **Untrusted**. Do not trust any CoS packet marking at ingress.
 - **802.1p**. The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of seven internal hardware priority queues. 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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 > CoS Interface Configuration**.

CoS		CoS Interface Configuration	
• Basic	▼	1 LAG All GO TO INTERFACE <input type="text"/> Go	
• Advanced	▲		
• CoS Configuration			
• CoS Interface Configuration			
• Interface Queue Configuration			
• 802.1p to Queue Mapping			
• DSCP to Queue Mapping			
<input type="checkbox"/>	Interface	Interface Trust Mode	Interface Shaping Rate (16 to 16384)
<input type="checkbox"/>	g1	802.1p	0
<input type="checkbox"/>	g2	802.1p	0
<input type="checkbox"/>	g3	802.1p	0
<input type="checkbox"/>	g4	802.1p	0
<input type="checkbox"/>	g5	802.1p	0
<input type="checkbox"/>	g6	802.1p	0
<input type="checkbox"/>	g7	802.1p	0
<input type="checkbox"/>	g8	802.1p	0
<input type="checkbox"/>	g9	802.1p	0
<input type="checkbox"/>	g10	802.1p	0
<input type="checkbox"/>	g11	802.1p	0

6. Click the **LAG** link to display all LAG interfaces or click the **All** link to display both all physical and all LAG interfaces.

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.** The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of seven internal hardware priority queues. The default 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 bandwidth allowed.

This is typically used to shape the outbound transmission rate in increments of 64 kbps in the range 16 to 16384 kbps. This value is controlled independently of any per-queue maximum bandwidth configuration. It is effectively a second-level shaping mechanism. The default is 0. The value 0 means that the maximum is unlimited.

The expected shaping at egress interface is calculated as follows:

$\text{frameSize} \times \text{shaping} / (\text{frameSize} + \text{IFG})$, where IFG (Inter frame gap) is 20 bytes, frameSize is configured frame size, and shaping is configured traffic shaping.

For example, when 64 bytes frame size and 64 kbps shaping are configured, expected shaping is approximately 48 kbps.

10. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

CoS		Interface Queue Configuration				
<ul style="list-style-type: none"> • Basic v • Advanced ^ <ul style="list-style-type: none"> • CoS Configuration • CoS Interface Configuration • Interface Queue Configuration • 802.1p to Queue Mapping • DSCP to Queue Mapping 		1 LAG All		GO TO INTERFACE <input type="text"/> <input type="button" value="Go"/>		
<input type="checkbox"/>	Interface	Queue ID	Minimum Bandwidth (0 to 100)	Scheduler Type	Queue Management Type	
		0 v	0 <input type="text"/>	<input type="text"/> v		
<input type="checkbox"/>	g1	0	0	Weighted	Taildrop	
<input type="checkbox"/>	g2	0	0	Weighted	Taildrop	
<input type="checkbox"/>	g3	0	0	Weighted	Taildrop	
<input type="checkbox"/>	g4	0	0	Weighted	Taildrop	
<input type="checkbox"/>	g5	0	0	Weighted	Taildrop	
<input type="checkbox"/>	g6	0	0	Weighted	Taildrop	
<input type="checkbox"/>	g7	0	0	Weighted	Taildrop	
<input type="checkbox"/>	g8	0	0	Weighted	Taildrop	
<input type="checkbox"/>	g9	0	0	Weighted	Taildrop	
<input type="checkbox"/>	g10	0	0	Weighted	Taildrop	
<input type="checkbox"/>	g11	0	0	Weighted	Taildrop	

6. Click the **LAG** link to display all LAG interfaces or click the **All** link to display both all physical and all LAG interfaces.
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.
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 is 0. The valid 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**. Services traffic with the highest priority on a queue first.
 - **Weighted**. Weighted round robin associates 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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

802.1p to Queue Mapping

You can view and 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

CoS		802.1p to Queue Mapping								
▫ Basic	▼	802.1p Priority	0	1	2	3	4	5	6	7
▫ Advanced	▲	Queue	1 ▼	0 ▼	2 ▼	3 ▼	4 ▼	5 ▼	6 ▼	7 ▼
▫ CoS Configuration										
▫ CoS Interface Configuration										
▫ Interface Queue Configuration										
▫ 802.1p to Queue Mapping										
▫ DSCP to Queue Mapping										

6. In the 802.1p to Queue Mapping table, map each of the eight 802.1p priorities to a queue (internal traffic class).

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 (7). For example, traffic with a priority of 0 is for most data traffic and is sent using best effort. Traffic with a higher priority, such as 7, 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.

7. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

DSCP to Queue Mapping

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 [Change the Default IP Address of the Switch](#) on page 9.

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 > DSCP to Queue Mapping**.

CoS		Class Selector (CS) PHB							
Basic	▼	DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
Advanced	▲	CS 0 (000000)	2 ▼	CS 2 (010000)	1 ▼	CS 4 (100000)	4 ▼	CS 6 (110000)	6 ▼
CoS Configuration		CS 1 (001000)	0 ▼	CS 3 (011000)	3 ▼	CS 5 (101000)	5 ▼	CS 7 (111000)	7 ▼
CoS Interface Configuration		Assured Forwarding (AF) PHB							
Interface Queue Configuration		DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
802.1p to Queue Mapping		AF 11 (001010)	0 ▼	AF 21 (010010)	1 ▼	AF 31 (011010)	3 ▼	AF 41 (100010)	4 ▼
DSCP to Queue Mapping		AF 12 (001100)	0 ▼	AF 22 (010100)	1 ▼	AF 32 (011100)	3 ▼	AF 42 (100100)	4 ▼
		AF 13 (001110)	0 ▼	AF 23 (010110)	1 ▼	AF 33 (011110)	3 ▼	AF 43 (100110)	4 ▼

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, apart from 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.

7. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 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. 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. Conversely, any degradation of service can negatively affect applications with strict timing requirements, such as voice or multimedia.

DiffServ Configuration Overview

To use DiffServ for QoS, you must enable DiffServ (see *Enable the DiffServ Mode and View the DiffServ Status* on page 161) and define the following categories and their criteria:

1. **Class.** Create classes and define class criteria (see *Configure a DiffServ Class* on page 163).
2. **Policy.** Create policies, associate classes with policies, and define policy statements (see *Configure a DiffServ Policy* on page 168).
3. **Service.** Add a policy to an inbound interface (see *Configure the DiffServ Service Interface* on page 174).

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.

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

Configure DiffServ Settings

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.

Enable the DiffServ Mode and View the DiffServ Status

You can enable the DiffServ mode and view the 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.

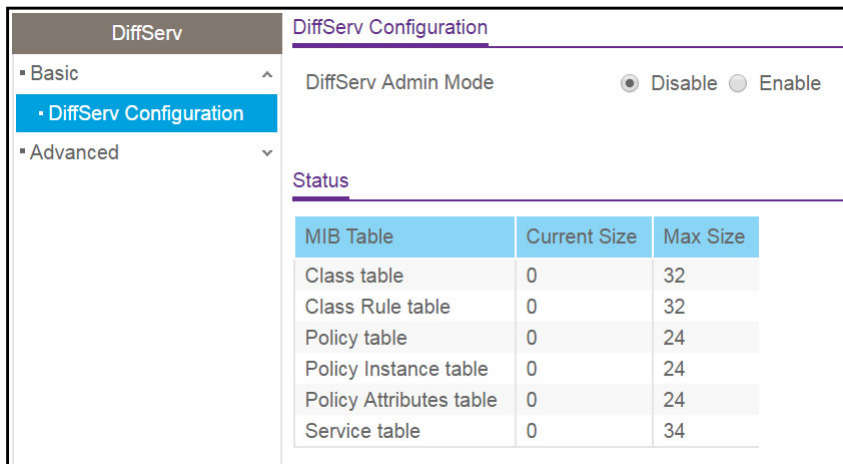
➤ To enable the DiffServ mode and view the DiffServ status

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 [Change the Default IP Address of the Switch](#) on page 9.
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 > Basic > DiffServ Configuration**.



6. Select the administrative mode for DiffServ:
 - **Enable**. Differentiated services are active.
 - **Disable**. The DiffServ configuration is retained and can be changed but is not active.
7. Click the **Apply** button.
The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information on the page.

Table 37. DiffServ Status information

Field	Description
Class table	The number of configured DiffServ classes out of the total allowed on the switch.
Class Rule table	The number of configured class rules out of the total allowed on the switch.
Policy table	The number of configured policies out of the total allowed on the switch.
Policy Instance table	The number of configured policy class instances out of the total allowed on the switch.

Table 37. DiffServ Status information (continued)

Field	Description
Policy Attributes table	The number of configured policy attributes (attached to the policy class instances) out of the total allowed on the switch.
Service table	The number of configured services (attached to the policies on specified interfaces) out of the total allowed on the switch.

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.

Create and Configure a DiffServ Class

➤ **To create 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

DiffServ	Class Configuration	
▪ Basic	<input type="checkbox"/>	Class Name
▪ Advanced		Class Type
▪ DiffServ Configuration	<input type="text"/>	<input type="text"/>
▪ Class Configuration		
▪ Policy Configuration		
▪ Service Configuration		
▪ Service Statistics		

6. In the **Class Name** field, enter a class name.

The **Class Name** field also lists all the existing DiffServ class names, from which one can be selected for modification or deletion.

- From the **Class Type** menu, select the class type.

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. You can select the class type only when you are creating a new class. After the class is created, the **Class Type** field becomes nonconfigurable.

- Click the **Add** button.

The new class is added.

- 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.

The screenshot displays the configuration interface for a DiffServ class. On the left is a navigation menu with 'DiffServ' at the top, followed by 'Basic', 'Advanced', 'DiffServ Configuration', 'Class Configuration' (highlighted), 'Policy Configuration', 'Service Configuration', and 'Service Statistics'. The main area is divided into two sections: 'Class Information' and 'Diffserv Class Configuration'.
 In the 'Class Information' section, 'Class Name' is set to 'Class1' and 'Class Type' is set to 'All'.
 The 'Diffserv Class Configuration' section features a list of radio buttons for match criteria: 'Match Every' (selected), 'Reference Class', 'Class of Service', 'VLAN', 'Ethernet Type', 'Source MAC', 'Destination MAC', 'Protocol Type', 'Source IP Address', 'Source L4 Port', 'Destination IP Address', 'Destination L4 Port', 'IP DSCP', 'Precedence Value', and 'IP ToS'.
 Under 'Match Every', there is a dropdown menu currently set to 'Any'. Below this are various input fields for defining match criteria, including:
 - 'Reference Class': 'No Reference Class Present'
 - 'VLAN': A text box with '(1 to 4093)' next to it.
 - 'Ethernet Type': A dropdown menu and a text box with '(600 to ffff hex)' next to it.
 - 'Source IP Address': 'Address' field, '0' in a text box, and '(0 to 255)' next to it, with a 'Mask' field.
 - 'Source L4 Port': A dropdown menu, '0' in a text box, and '(0 to 65535)' next to it, with a 'Mask' field.
 - 'Destination IP Address': 'Address' field, '0' in a text box, and '(0 to 255)' next to it, with a 'Mask' field.
 - 'Destination L4 Port': A dropdown menu, '0' in a text box, and '(0 to 65535)' next to it, with a 'Mask' field.
 - 'IP DSCP': A dropdown menu, '0' in a text box, and '(0 to 63)' next to it.
 - 'Precedence Value': A text box with '0' and '(0 to 7)' next to it.
 - 'IP ToS': 'Bit Value' field and a text box with '0' and '(0 to 7)' next to it, with a 'Bit Mask' field.

- Define the criteria that must be associated the DiffServ class:

- 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 at most 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 one can be selected.

- **VLAN.** Select this radio button to require a packet's VLAN ID to match a VLAN ID or a VLAN ID within a continuous range. If you configure a range, a match occurs if a packet's VLAN ID is the same as any VLAN ID within the range. The VLAN value is in the range of 1–4093.
- **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, specify the EtherType keyword from the list of common protocols that are mapped to their Ethertype value.
- **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.
 - **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.
 - **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. The menu includes **Other** as a selection, which lets you 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. The menu includes **Other** as a selection, which lets you enter a source port number.

- **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, which you must select from the menu. The menu includes **Other** as a selection, which lets you enter a destination port number.
- **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. The menu includes **Other** as a selection, which lets you 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.

11. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information on the page.

Table 38. DiffServ Class Configuration, Class Summary information

Field	Description
Match Criteria	The configured match criteria for the specified class.
Values	The values of the configured match criteria.

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 [Change the Default IP Address of the Switch](#) on page 9.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 class with a policy.

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

DiffServ		Policy Configuration			
▪ Basic	▼	<input type="checkbox"/>	Policy Name	Policy Type	Member Class
▪ Advanced	▲		<input type="text"/>		Class1 ▼
• DiffServ Configuration					
• Class Configuration					
• Policy Configuration					
• Service Configuration					
• Service Statistics					

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.

Class Information	
Policy Name	Premium
Policy Type	In
Member Class Name	Class1
Policy Attribute	
Policy Attribute	<input checked="" type="radio"/> Assign Queue <input type="text" value="0"/>
	<input type="radio"/> Drop
	<input type="radio"/> Mark VLAN CoS <input type="text" value="0"/>
	<input type="radio"/> Mark IP Precedence <input type="text" value="0"/>
	<input type="radio"/> Mark IP DSCP <input type="text" value="af11"/>
	<input type="radio"/> Simple Policy
Color Mode	ColorBlind
Committed Rate	<input type="text"/>
Conform Action	<input checked="" type="radio"/> Send
	<input type="radio"/> Drop
	<input type="radio"/> Mark CoS <input type="text" value="0"/>
	<input type="radio"/> Mark IP Precedence <input type="text" value="0"/>
	<input type="radio"/> Mark IP DSCP <input type="text" value="af11"/>
Violate Action	<input checked="" type="radio"/> Drop

10. From the **Assign Queue** menu, select the queue to which packets of this policy class must be assigned.

This is an integer value in the range 0 to 7.

11. Configure the policy attributes:

- **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 an integer 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.
- **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 menu includes **Other** as a selection, which lets you 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.
- **Simple Policy.** Select this radio button to define the traffic policing style for the class. A simple policy uses a single data rate and burst size, resulting in one of two outcomes: conform or violate. You must define the policy as described in the next step.

12. If you select the **Simple Policy** radio button, you can specify the traffic policing style for the class:

- **Color Mode.** From the menu, select one of the following options:
 - **Color Blind.** This is the default selection. Color classes do not apply.

Note: A valid color class contains a single, non-excluded match criterion for the CoS, IP DSCP, or IP Precedence option. The configured option must not conflict with the classifier of the policy instance itself.

- **Committed Rate.** Enter the committed rate that is applied to conforming packets by specifying a value in the range from 1 to 65535.b

The switch multiplies the value that you enter by 16 to get the value in kb/s.

13. Select the conforming actions.

The Conform Action section lists the actions to be taken on conforming packets according to the policing metrics. By default, conforming packets are sent.

In the Conform Action section, select one of the following actions:

- **Send.** Packets are forwarded unmodified. This is the default conforming action and 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 select a DSCP code from the menu. The menu includes **Other** as a selection, which lets you enter an IP DSCP value from 0 to 63. The DSCP value is defined as the high-order six bits of the Service Type octet in the IP header.

Note: In the Violate Action section, by default the **Drop** radio button is selected. No other selection is available because the switch always drops packets that violate the policy.

14. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information on the page.

Table 39. DiffServ policy configuration policy attributes

Field	Description
Policy Name	Displays the name of the DiffServ policy.
Policy Type	Displays type of the policy as In.
Member Class Name	Displays the name of the class instance within the policy.

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 [Change the Default IP Address of the Switch](#) on page 9.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.
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.
The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.
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 activate a policy on 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

DiffServ		Service Interface Configuration		
Basic	▼	1 LAG All		
Advanced	▲	Go To Interface <input type="text"/> <input type="button" value="Go"/>		
DiffServ Configuration		<input type="checkbox"/>	Interface	Policy In Name
Class Configuration				Direction
Policy Configuration				Operational Status
Service Configuration				
Service Statistics				
			Premium ▼	
		<input type="checkbox"/>	g1	
		<input type="checkbox"/>	g2	
		<input type="checkbox"/>	g3	
		<input type="checkbox"/>	g4	
		<input type="checkbox"/>	g5	
		<input type="checkbox"/>	g6	
		<input type="checkbox"/>	g7	
		<input type="checkbox"/>	g8	
		<input type="checkbox"/>	g9	
		<input type="checkbox"/>	g10	
		<input type="checkbox"/>	g11	

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 **Policy Name** menu, select a policy name.
8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information on the page.

Table 40. Service Interface Configuration information

Field	Description
Direction	Shows that the traffic direction of this service interface is In.
Operational Status	Shows the operational status of this service interface, either Up or Down.

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 [Change the Default IP Address of the Switch](#) on page 9.
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.
The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

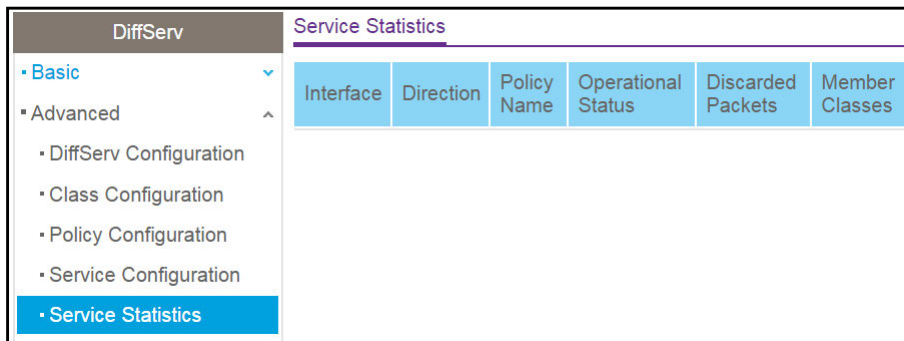
The login window opens.

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**.



6. Click the **Update** button to refresh the page with the latest information about the switch.

The following table describes the nonconfigurable information on the page.

Table 41. DiffServ Service Statistics information

Field	Description
Interface	List of all valid slot number and port number combinations on the switch with a DiffServ policy currently attached in the inbound direction.
Direction	List of the traffic direction of interface as In. Shows only the directions for which a DiffServ policy is currently attached.
Policy Name	Name of the policy currently attached to the specified interface and direction.
Operational Status	Operational status of the policy currently attached to the specified interface and direction. The value is either Up or Down.

Table 41. DiffServ Service Statistics information (continued)

Field	Description
Discarded Packets	A count of the total number of packets discarded for all class instances in this service policy for any reason due to DiffServ treatment. This is the overall count per interface, per direction. The discarded packets are supported in the inbound direction but not in the outbound direction.
Member Classes	List of all DiffServ classes currently 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 nothing is populated in the list.

5. Manage Device Security

5

This chapter contains the following sections:

- *Configure the Management Security Settings*
- *Configure Management Access*
- *Configure Port Authentication*
- *Configure 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

You can change the login password.

➤ **To change the login password for the management 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 [Change the Default IP Address of the Switch](#) on page 9.

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 > User Configuration > Change Password**.

Management Security	Change Password	
• User Configuration ^	Old Password	<input type="password"/> (1 to 20)
• Change Password	New Password	<input type="password"/> (1 to 20)
• RADIUS v	Confirm Password	<input type="password"/> (1 to 20)
• TACACS+ v	Reset Password	<input type="checkbox"/>
• Authentication List v		

6. In the **Old Password** field, specify the current password for the account created by the user.

The entered password is displayed in dots. Passwords are up to 20 alphanumeric characters in length, and are case sensitive.

7. In the **New Password** field, specify the optional new or changed password for the account.

The entered password is displayed in dots. Passwords are up to 20 alphanumeric characters in length, and are case sensitive.

8. In the **Confirm Password** field, enter the password again to confirm that you entered it correctly.

The entered password is displayed in dots.

9. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Note: If you forget the password and are unable to log in to the switch management 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.

Configure RADIUS Servers

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.

Consider the maximum delay time when you are configuring RADIUS maximum retransmit and RADIUS time-out values. If multiple RADIUS servers are configured, the maximum retransmit period on each server runs out before the next server is attempted. A retransmit does not occur until the configured time-out period on that server passes without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the retransmit time x time-out period for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the RADIUS application returns a 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Management Security	RADIUS Configuration	
• User Configuration	Current Server IP Address	
• RADIUS	Number of Configured Servers	0
• Global Configuration	Max Number of Retransmits	<input type="text" value="4"/> (1 to 15)
• Server Configuration	Timeout Duration (secs)	<input type="text" value="5"/> (1 to 30)
• Accounting Server Configuration	Accounting Mode	Disable ▾
• TACACS+		
• Authentication List		

The Current Server IP Address field is blank if no servers are configured (see [Configure a RADIUS Authentication Server on the Switch](#) on page 182). 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.

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

The valid range is from 1 to 15. The default is 4.

Consider the maximum delay time when you are configuring RADIUS maximum retransmit and RADIUS time-out values. If multiple RADIUS servers are configured, the maximum retransmit period on each server runs out before the next server is attempted. A retransmit does not occur until the configured time-out period on that server passes without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the retransmit time x time-out period for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the RADIUS application returns a response.

7. In the **Timeout Duration** field, specify the time-out value, in seconds, for request retransmissions.

The valid range is from 1 to 30. The default is 5.

Consider the maximum delay time when you are configuring RADIUS maximum retransmit and RADIUS time-out values. If multiple RADIUS servers are configured, the maximum retransmit period on each server runs out before the next server is attempted. A retransmit does not occur until the configured time-out period on that server passes without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the retransmit time x time-out period for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the RADIUS application returns a response.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information on the page.

Table 42. RADIUS Configuration information

Field	Description
Current Server Address	The address of the current server. This field is blank if no servers are configured.
Number of Configured Authentication Servers	The number of configured authentication RADIUS servers. The value can range from 0 to 32.

Configure a RADIUS Authentication Server on the Switch

You can 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 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 [Change the Default IP Address of the Switch](#) on page 9.
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**.

Server Configuration						
<input type="checkbox"/>	Server Address	Authentication Port	Secret Configured	Secret	Active	Message Authenticator
	<input type="text"/>	1812	<input type="text"/>	<input type="text"/>	Primary	Disable

Statistics												
Server Address	Round Trip Time	Access Requests	Access Retransmissions	Access Accepts	Access Rejects	Access Challenges	Malformed Access Responses	Bad Authenticators	Pending Requests	Timeouts	Unknown Types	Packets Dropped

- In the **Server Address** field, specify the IP address of the RADIUS server.
- In the **Authentication Port** field, specify the UDP port number the server uses to verify the RADIUS server authentication.

The valid range is from 1 to 65535. The default is 1812.

- 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.
- In the **Secret** field, type the shared secret text string used for authenticating and encrypting all RADIUS communications between the switch and the RADIUS server.

This secret must match the RADIUS encryption.

- From the **Active** menu, select **Primary**.
- 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.

- Click the **Add** button.

The server is added to the switch.

- Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information in the Statistics table on the page.

Field	Description
Server Address	The address of the RADIUS server or the name of the RADIUS server for which the statistics are displayed.
Round Trip Time	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.

Field	Description
Access Requests	The number of RADIUS access-request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS access-request packets retransmitted to this server.
Access Accepts	The number of RADIUS access-accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS access-reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS access-challenge packets, including both valid and invalid packets, that were received from this server.
Malformed Access Responses	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.
Bad Authenticators	The number of RADIUS access-response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS access-request packets destined for this server that did not yet time out or receive a response.
Timeouts	The number of authentication time-outs to this server.
Unknown Types	The number of RADIUS packets of unknown type that were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

14. To reset the authentication server and RADIUS statistics to their default values, click the **Clear Counters** button.

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 *Change the Default IP Address of the Switch* on page 9.

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**.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Remove a RADIUS Authentication Server From the Switch

- **To a 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 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 [Change the Default IP Address of the Switch](#) on page 9.

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 following figure does not show the Accounting Server Statistics section.

Management Security	Accounting Server Configuration	
• User Configuration	Accounting Server Address	<input type="text"/>
• RADIUS	Port	<input type="text" value="1813"/>
• Global Configuration	Secret Configured	<input type="text" value="No"/>
• Server Configuration	Secret	<input type="text"/>
• Accounting Server Configuration	Accounting Mode	<input type="text" value="Disable"/>
• TACACS+		

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 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.
You must select **Yes** before you can configure the RADIUS secret. After you add the RADIUS accounting server, this field indicates whether the shared secret for this server 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. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

13. The following table describes the nonconfigurable information in the Accounting Server Statistics table on the page.

Field	Description
Accounting Server Address	The accounting server associated with the statistics.
Round Trip Time (secs)	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.
Accounting Requests	The number of RADIUS accounting-request packets sent not including retransmissions.
Accounting Retransmissions	The number of RADIUS accounting-request packets retransmitted to this RADIUS accounting server.
Accounting Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Accounting Responses	The number of malformed RADIUS accounting-response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS accounting-response packets that contained invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS accounting-request packets sent to this server that did not yet time out or receive a response.
Timeouts	The number of accounting time-outs to this server.
Unknown Types	The number of RADIUS packets of unknown type that were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets that were received from this server on the accounting port and dropped for some other reason.

14. To reset the accounting server and RADIUS statistics to their default values, click the **Clear Counters** button.

Modify the Settings for a RADIUS Accounting Server on the Switch

➤ **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 [Change the Default IP Address of the Switch](#) on page 9.

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. Modify the configuration for the selected accounting server.

8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Remove a RADIUS Accounting Server From the Switch

➤ **To a 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 [Change the Default IP Address of the Switch](#) on page 9.

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. Click the **Delete** button.

The RADIUS accounting server is removed.

7. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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

The TACACS+ Configuration page contains the TACACS+ settings for communication between the switch and the TACACS+ server that you configure.

➤ 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 [Change the Default IP Address of the Switch](#) on page 9.

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+ Configuration**.

TACACS+ Configuration	
Key String	<input type="text"/> (0 to 128)
Connection Timeout	5 <input type="text"/> (1 to 30)

- In the **Key String** field, specify the authentication and encryption key for TACACS+ communications between the switch and the TACACS+ server.
The valid range is 0–128. The key must match the key configured on the TACACS+ server.
- In the **Connection Timeout** field, specify the maximum number of seconds allowed to establish a TCP connection between the switch and the TACACS+ server.
- Click the **Apply** button.
The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure a TACACS+ Server on the Switch

You can configure up to five TACACS+ servers with which the switch can communicate.

➤ To configure a TACACS+ server on the switch:

- 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.
- Launch a web browser.
- 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 [Change the Default IP Address of the Switch](#) on page 9.
The login window opens.
- Enter the switch's password in the **Password** field.
The default password is **password**.
The System Information page displays.
- Select **Security > Management Security > TACACS+ > TACACS+ Server Configuration**.

TACACS Server Configuration					
<input type="checkbox"/>	TACACS Server	Priority(0 to 65535)	Port(0 to 65535)	Key String	Connection Timeout(1-30)
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

- In the **TACACS+ Server** field, enter the TACACS+ server IP address.
- 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 valid range is 0–65535.

8. In the **Port** field, specify the authentication port value for TACAS+ server sessions. It must be within the range 0–65535. 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 valid range is 0–128. 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 1–30. If you do not specify a value, the switch uses a default of 5.

11. Click the **Add** button.

The server is added to the switch.

12. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure Authentication Lists

You can configure the default login list. A login list specifies one or more authentication methods to validate switch or port access for the admin user.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 > HTTP Authentication List**.

Management Security	HTTP Authentication List				
<ul style="list-style-type: none"> ▪ User Configuration ▾ ▪ RADIUS ▾ ▪ TACACS+ ▾ ▪ Authentication List ▾ <ul style="list-style-type: none"> • HTTP Authentication List • HTTPS Authentication List 	List Name	1	2	3	4
<input type="checkbox"/>	httpList	Local ▾	▾	▾	▾

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.
 - **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. This option is available only for Method 2 and Method 3.
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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

The screenshot shows the Management Security configuration page. The left sidebar has a tree view with the following items: Management Security (selected), User Configuration, RADIUS, TACACS+, Authentication List (expanded), HTTP Authentication List, and HTTPS Authentication List (selected). The main content area is titled 'HTTPS Authentication List' and contains a table with the following structure:

List Name	1	2	3	4
<input type="checkbox"/> httpsList	Local			

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.
- **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. This option is only available for Method 2 and Method 3.
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.
The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure Management Access

You can configure HTTP and secure HTTP access to the switch management interface. You can also configure access control profiles and access rules.

Configure HTTP Settings

You can configure the HTTP settings on the switch.

➤ To configure the HTTP 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 [Change the Default IP Address of the Switch](#) on page 9.
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**.

Access	HTTP Configuration	
▫ HTTP ^	HTTP Session Soft Timeout (Minutes)	<input type="text" value="60"/> (0 to 60)
▫ HTTP Configuration	HTTP Session Hard Timeout (Hours)	<input type="text" value="24"/> (0 to 168)
▫ HTTPS v	Maximum Number of HTTP Sessions	<input type="text" value="4"/> (1 to 4)
▫ Access Control v		

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 of 0–60 minutes. The default is 5 minutes. The currently configured value is shown when the web page is displayed.

After the session is inactive for the configured time, you are automatically logged out and must reenter the password to access the management 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 of 0–168 hours. value of zero means that the session does not time out. The default 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.

9. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure HTTPS 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.

You can configure the settings for HTTPS communication between the management station and the switch.

➤ **To configure HTTPS 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 [Change the Default IP Address of the Switch](#) on page 9.

The login window opens.

- Enter the switch's password in the **Password** field.

The default password is **password**.

The System Information page displays.

- Select **Security > Access > HTTPS > HTTPS Configuration**.

Access	HTTPS Configuration	
• HTTP	Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
• HTTPS	TLS Version 1	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
• HTTPS Configuration	HTTPS Port	<input type="text" value="443"/> (1025 to 65535) Default: 443
• Certificate Management	HTTPS Session Soft Timeout (Minutes)	<input type="text" value="5"/> (1 to 60)
• Certificate Download	HTTPS Session Hard Timeout (Hours)	<input type="text" value="24"/> (1 to 168)
• Access Control	Maximum Number of HTTPS Sessions	<input type="text" value="2"/> (0 to 4)

- Select the HTTPS Admin Mode **Enable** or **Disable** radio button.

This enables or disables the administrative mode of secure HTTP (HTTPS). The configured value is displayed. The default is Disable. You can download SSL certificates only when the HTTPS admin mode is disabled. HTTPS admin mode can be enabled only if a certificate is present on the device.

- Select the TLS Version 1 **Enable** or **Disable** radio button.

This enables or disables Transport Layer Security version 1.0. The configured value is displayed. The default is Enable.

- In the **HTTPS Port** field, type the HTTPS port number.

The value must be in the range of 1025 to 65535. Port 443 is the default port. The configured value is displayed.

- In the **HTTPS Session Soft Timeout (Minutes)** field, enter the inactivity time-out for HTTPS sessions.

The value must be in the range of 1 to 60 minutes. The default is 5 minutes. The configured value is displayed.

- 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 value must be in the range of 1 to 168 hours. The default is 24 hours.

- In the **Maximum Number of HTTPS Sessions** field, enter the maximum allowable number of HTTPS sessions.

The value must be in the range of 0 to 4. The default is 4.

- Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Manage Certificates

You can manage certificates.

Generate an SSL Certificate

➤ **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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Access	Certificate Management
• HTTP	Certificate Present Yes
• HTTPS	<input checked="" type="radio"/> None
• HTTPS Configuration	<input type="radio"/> Generate Certificates
• Certificate Management	<input type="radio"/> Delete Certificates
• Certificate Download	
• Access Control	
	Certificate Generation Status
	Certificate Generation Status No certificate generation in progress

The **Certificate Present** field displays whether a certificate is present on the switch.

6. In the Certificate Management area, select **Generate Certificates**.

7. Click the **Apply** button.

The switch generates an SSL certificate.

The Certificate Generation Status field shows information about the progress.

Delete an SSL Certificate

➤ 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 *Change the Default IP Address of the Switch* on page 9.
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**.
6. The Certificate Management page displays.
The Certificate Present field displays Yes.
7. In the Certificate Management area, select **Delete Certificates**.
8. Click the **Apply** button.
The certificate is removed.

Download Certificates

You can transfer a certificate file to the switch.

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

➤ To configure the certificate download 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

The screenshot shows the 'Certificate Download' configuration page. On the left is a navigation tree under 'Access' with 'Certificate Download' selected. The main area contains the following fields:

File Type	SSL Server Certificate PEM File
TFTP Server IP	0.0.0.0
Remote File Name	
Start File Transfer	<input type="checkbox"/>

Note: By default, the selection from the **File Type** menu is **SSL Server Certificate PEM File**. No other selection are available.

6. In the **TFTP Server IP** field, specify the address of the TFTP server.

The address can be an IP address in standard x.x.x.x format or a host name. The host name must start with a letter of the alphabet. Make sure that the software image or other file to be downloaded is available on the TFTP server.

7. 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.

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

9. Click the **Apply** button.

The file transfer starts. A status message displays during the transfer and upon successful completion of the transfer.

Configure Access Control

Access control allows you to configure a profile and set access rules.

Configure an Access Control Profile

You can set -up a security access profile.

➤ **To configure 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Access Profile Configuration

Access Profile Name

Activate Profile

Deactivate Profile

Remove Profile

Profile Summary

Rule Type	Service Type	Source IP Address	Mask	Priority
-----------	--------------	-------------------	------	----------

6. In the **Access Profile Name** field, enter the name of the access profile to be added.

The maximum length is 32 characters.

7. Select one of the following check boxes:

- **Activate Profile.** Activate an access profile.
- **Deactivate Profile.** Deactivate an access profile.
- **Remove Profile.** Remove an access profile. The access profile must be deactivated before you remove the access profile.

8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

9. To refresh the page with the latest information about the switch, click the **Update** button. The following table describes the nonconfigurable information on the page.

Table 43. Access profile configuration profile summary

Field	Description
Rule Type	The action performed when the rules are matched.
Service Type	The service type chosen. The policy is restricted by the service type chosen.
Source IP Address	Source IP address of the client originating the management traffic.
Mask	The subnet mask of the IP Address.
Priority	The priority of the rule.

Configure Access Rule Settings

You can add security access rules. You can apply changes to an access rule only when the access profile is in a deactivated state.

Note: You must create an access profile before you can add rules.

➤ To configure the access rule 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 [Change the Default IP Address of the Switch](#) on page 9.

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				
Rule Type	Service Type	Source IP Address	Mask	Priority
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<div style="border: 1px solid black; padding: 2px;"> HTTP Secure HTTP(SSL) SNMP </div>			

- 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 by traffic that matches the rule criteria. A Deny rule blocks traffic that matches the rule criteria.

- 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 **HTTP**, **Secure HTTP (SSL)**, and **SNMP**.

- In the **Source IP Address** field, enter the source IP address of the client originating the management traffic.
- In the **Mask** field, specify the subnet mask of the client that originates the management traffic.
- 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 are ignored. For example, if a source IP 10.10.10.10 is configured with priority 1 to permit, and source IP 10.10.10.10 is configured with priority 2 to deny, then access is permitted if the profile is active, and the second rule is ignored.

- Click the **Add** button.

The access rule is added.

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 given time, only one supplicant is allowed to attempt authentication on a port in this mode. Ports in this mode are under bidirectional control. This is the default authentication mode.

An 802.1X network includes three components:

- **Authenticators.** The port that is authenticated before system access is permitted.
- **Supplicants.** The host 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 user 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 all 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 [Change the Default IP Address of the Switch](#) on page 9.

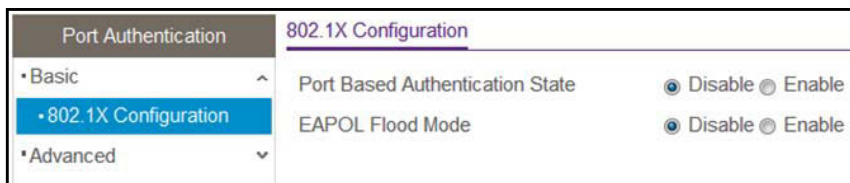
The login window opens.

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. Next to Port Based Authentication State, select the **Enable** radio button.

This enables or disables 802.1X administrative mode on the switch.

Note: 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 191.

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.

7. Next to EAPOL Flood Mode, select the **Enable** radio button.

The default is Disable. Extensible Authentication Protocol (EAP) over LAN (EAPoL) flood support is enabled on the switch.

8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Manage Port Authentication

You can enable and configure port access control on one or more 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 [Change the Default IP Address of the Switch](#) on page 9.

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 following figure does not show all columns on the page.

Port	Port Control	Guest VLAN ID	Guest VLAN Period	Periodic Reauthentication	Reauthentication Period	Quiet Period	Resending EAP	Max EAP Requests	Supplicant Timeout	Server Timeout	Control Direction	Protocol Version	PAE Capabilities	Authenticator PAE State
<input type="checkbox"/> g1	Auto	0	90	Disable	3600	60	30	2	30	30	Both	1	Authenticator	Initialize
<input type="checkbox"/> g2	Auto	0	90	Disable	3600	60	30	2	30	30	Both	1	Authenticator	Initialize
<input type="checkbox"/> g3	Auto	0	90	Disable	3600	60	30	2	30	30	Both	1	Authenticator	Initialize
<input type="checkbox"/> g4	Auto	0	90	Disable	3600	60	30	2	30	30	Both	1	Authenticator	Initialize
<input type="checkbox"/> g5	Auto	0	90	Disable	3600	60	30	2	30	30	Both	1	Authenticator	Initialize
<input type="checkbox"/> g6	Auto	0	90	Disable	3600	60	30	2	30	30	Both	1	Authenticator	Initialize
<input type="checkbox"/> g7	Auto	0	90	Disable	3600	60	30	2	30	30	Both	1	Authenticator	Initialize
<input type="checkbox"/> g8	Auto	0	90	Disable	3600	60	30	2	30	30	Both	1	Authenticator	Initialize
<input type="checkbox"/> g9	Auto	0	90	Disable	3600	60	30	2	30	30	Both	1	Authenticator	Initialize
<input type="checkbox"/> g10	Auto	0	90	Disable	3600	60	30	2	30	30	Both	1	Authenticator	Initialize
<input type="checkbox"/> g11	Auto	0	90	Disable	3600	60	30	2	30	30	Both	1	Authenticator	Initialize
<input type="checkbox"/> g12	Auto	0	90	Disable	3600	60	30	2	30	30	Both	1	Authenticator	Initialize

6. Select the check box next to the port.

You can also select multiple check boxes to apply the same settings to the selected ports, or select the check box in the heading row to apply the same settings to all ports.

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 system automatically detects the mode of the interface.
 - **Authorized.** The system places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication.

- **Unauthorized.** The system 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.
 - **MAC based.** This mode allows multiple supplicants connected to the same port to each authenticate individually. Each host connected to the port must authenticate separately in order to gain access to the network. The hosts are distinguished by their MAC addresses.
 - **Guest VLAN ID.** Specify the VLAN ID for the guest VLAN. The valid range is 0–4093. The default 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.
 - **Guest VLAN Period.** Specify the number of seconds that the selected port remains in the quiet state following a failed authentication exchange. The guest VLAN time-out must be a value in the range of 1–300. The default is 90.
 - **Periodic Reauthentication.** Select **Enable** to allow periodic reauthentication of the supplicant for the specified port.
 - **Reauthentication Period.** Specify the time, in seconds, after which reauthentication of the supplicant occurs. The reauthentication period must be a value in the range of 1–65535. The default is 3600. If this field is disabled, connected clients are not forced to reauthenticate periodically.
 - **Quiet Period.** Specify the number of seconds that the port remains in the quiet state following a failed authentication exchange. While in the quiet 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 value, 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 selected 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 selected port. The supplicant time-out is the value, 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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information on the page.

Table 44. Port authentication status information

Field	Description
Control Direction	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).
Protocol Version	The protocol version associated with the selected port. The only possible value is 1, corresponding to the first version of the 802.1X specification.
PAE Capabilities	The port access entity (PAE) functionality of the selected port. Possible values are Authenticator or Supplicant.
Authenticator PAE State	The current state of the authenticator PAE state machine. Possible values are as follows: Initialize Disconnected Connecting Authenticating Authenticated Aborting Held ForceAuthorized ForceUnauthorized
Backend State	The current state of the backend authentication state machine. Possible values are as follows: Request Response Success Fail Timeout Initialize Idle

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 [Change the Default IP Address of the Switch](#) on page 9.

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.

Restart the 802.1X Authentication Process on a Port

- **To restart the 802.1X authentication process 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 [Change the Default IP Address of the Switch](#) on page 9.

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 reauthenticate.

7. Click the **Reauthenticate** button.

The selected port is forced to restart the authentication process. This button is available only if the control mode is auto. If the button is not selectable, it is grayed out. 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 [Change the Default IP Address of the Switch](#) on page 9.

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 Summary**.

Port Authentication		Port Summary			
<ul style="list-style-type: none"> ▪ Basic ▪ Advanced <ul style="list-style-type: none"> • 802.1X Configuration • Port Authentication • Port Summary 		1			
Port	Control Mode	Operating Control Mode	Reauthentication Enabled	Port Status	
g1	Auto	Auto	False	Authorized	
g2	Auto	Auto	False	Authorized	
g3	Auto	Auto	False	Authorized	
g4	Auto	Auto	False	Authorized	
g5	Auto	Auto	False	Authorized	
g6	Auto	Auto	False	Authorized	
g7	Auto	Auto	False	Authorized	
g8	Auto	Auto	False	Authorized	
g9	Auto	Auto	False	Authorized	
g10	Auto	Auto	False	Authorized	
g11	Auto	Auto	False	Authorized	
g12	Auto	Auto	False	Authorized	

The following table describes the nonconfigurable information on the page.

Table 45. Port summary

Field	Description
Port	The port for which the settings are displayed in the table row.
Control Mode	<p>This field indicates the configured control mode for the port. Possible values are as follows:</p> <ul style="list-style-type: none"> • Force Unauthorized. The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized. • Force Authorized. The authenticator PAE unconditionally sets the controlled port to authorized. • Auto. The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server. • MAC Based. 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.
Operating Control Mode	<p>The control mode under which the port is actually operating. Possible values are as follows:</p> <ul style="list-style-type: none"> • ForceUnauthorized • ForceAuthorized • Auto • MAC Based • N/A: If the port is in detached state, it cannot participate in port access control.
Reauthentication Enabled	This field shows whether reauthentication of the supplicant for the specified port is allowed. The possible values are True and False. If the value is True, reauthentication occurs. Otherwise, reauthentication is not allowed.
Port Status	The authorization status of the specified port. The possible values 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.

Configure Traffic Control

You can configure MAC filters, storm control, port security, protected port, and private VLAN settings.

Manage MAC Filtering

You can create MAC filters that limit the traffic that is allowed into specified ports on the switch.

Create a MAC 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 [Change the Default IP Address of the Switch](#) on page 9.

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 screenshot shows the 'MAC Filter Configuration' page. On the left is a sidebar with 'Traffic Control' expanded to 'MAC Filter Configuration'. The main content area includes:

- MAC Filter:** A dropdown menu set to 'Create Filter'.
- VLAN ID:** A text input field containing the number '1'.
- MAC Address:** An empty text input field.
- Source Port Members:** A section titled 'Unit 1' containing a grid of 26 port icons labeled 1 through 26.
- LAG:** A section titled 'LAG' containing a grid of 8 port icons labeled 1 through 8.

- From the **MAC Filter** menu, select **Create Filter**.

If you did not configure any filters, this is the only option available.

- From the **VLAN ID** menu, select the VLAN that must be used with the MAC address.
- 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

- 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.

- Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Delete a MAC Filter

➤ To delete a MAC filter:

- 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.

- Launch a web browser.
- 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 [Change the Default IP Address of the Switch](#) on page 9.

The login window opens.

- Enter the switch's password in the **Password** field.

The default password is **password**.

The System Information page displays.

- Select **Security > Traffic Control > MAC Filter > MAC Filter Configuration**.

The MAC Filter Configuration page displays.

- From the **MAC Filter** menu, select the filter.
- 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 [Change the Default IP Address of the Switch](#) on page 9.

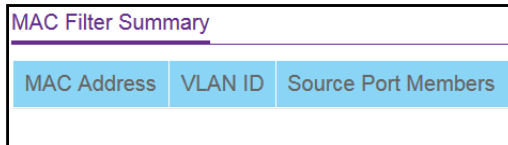
The login window opens.

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 Summary**.



MAC Filter Summary		
MAC Address	VLAN ID	Source Port Members

The following table describes the nonconfigurable information on the page.

Table 46. MAC Filter Summary information

Field	Description
MAC Address	The MAC address of the filter in the format XX:XX:XX:XX:XX:XX.
VLAN ID	The VLAN ID used with the MAC address to fully identify packets you want filtered.
Source Port Members	A list of ports to be used for filtering inbound packets.

Configure Storm Control

A broadcast storm is the result of an excessive number of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses can overload network resources, 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.

➤ **To configure 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Storm Control

Ingress Control Mode: Disable

Status: Disable

Threshold:

Control Action: Drop

Port Settings

Go To Interface: Go

<input type="checkbox"/>	Port	Status	Threshold	Control Action
<input type="checkbox"/>	g1	Disable		
<input type="checkbox"/>	g2	Disable		
<input type="checkbox"/>	g3	Disable		
<input type="checkbox"/>	g4	Disable		

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. In the Storm Control section, from the **Ingress Control Mode** menu, select the mode of broadcast affected by 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.
8. 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.
9. In the **Threshold** field, specify the maximum rate at which unknown packets are forwarded. The range is a percent of the total threshold between 0–100%. The default is 5%.
10. From the **Control Action** mode menu, select one of the following options:
 - **Drop.** If the threshold of the configured broadcast storm is exceeded, the packet is dropped. This is the default action.
 - **Shutdown.** If the threshold of the configured broadcast storm is exceeded, the port is shut down.
11. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure Port Security

Port security lets you lock one or more ports on the switch. When a port is locked, only packets with an allowable source MAC addresses can be forwarded. All other packets are discarded.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Port Security > Port Security Configuration**.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

8. Click the **Update** button to refresh the page with the latest information about the switch.

The Port Security Violations table shows information about violations that occurred on ports that are enabled for port security. The fields are described in the following table.

Table 47. Port Security Violations information

Field	Description
Port	The physical interface.
Last Violation MAC	The source MAC address of the last packet that was discarded at a locked port.
VLAN ID	The VLAN ID corresponding to the last MAC address violation.

Configure a Port Security Interface

A MAC address can be defined as allowable by one of two methods: dynamically or statically. Both methods are used concurrently when a port is locked.

Dynamic locking implements a first arrival mechanism for port security. You specify how many addresses can be learned on the locked port. If the limit was not reached, then a packet with an unknown source MAC address is learned and forwarded normally. When the limit is reached, no more addresses are learned on the port. Any packets with source MAC addresses that were not already learned are discarded. You can effectively disable dynamic locking by setting the number of allowable dynamic entries to zero.

Static locking allows you to specify a list of MAC addresses that are allowed on a port. The behavior of packets is the same as for dynamic locking: only packets with an allowable source MAC address can be forwarded.

➤ **To configure port security 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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Port Security > Interface Configuration**.

Traffic Control		Interface Configuration				
<ul style="list-style-type: none"> • MAC Filter • Storm Control • Port Security <ul style="list-style-type: none"> • Port Security Configuration • Interface Configuration • Security MAC Address • Protected Ports 		1 LAG All		Go To Port	<input type="text"/>	<input type="button" value="Go"/>
<input type="checkbox"/>	Port	Port Security	Max Learned MAC Address	Max Static MAC Address	Enable Violation Traps	
<input type="checkbox"/>	g1	Disable	600	20	No	
<input type="checkbox"/>	g2	Disable	600	20	No	
<input type="checkbox"/>	g3	Disable	600	20	No	
<input type="checkbox"/>	g4	Disable	600	20	No	
<input type="checkbox"/>	g5	Disable	600	20	No	
<input type="checkbox"/>	g6	Disable	600	20	No	
<input type="checkbox"/>	g7	Disable	600	20	No	
<input type="checkbox"/>	g8	Disable	600	20	No	
<input type="checkbox"/>	g9	Disable	600	20	No	
<input type="checkbox"/>	g10	Disable	600	20	No	
<input type="checkbox"/>	g11	Disable	600	20	No	

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 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.
 - **Max Static MAC Address.** Specify the maximum number of statically locked MAC addresses on the selected interfaces.
 - **Enable Violation Traps.** Enable or disable the sending of new violation traps if a packet with a disallowed MAC address is received. The default is No, which means that the option is disabled.
8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

View Learned MAC Addresses and Convert Them to Static MAC Addresses

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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Port Security > Port Security Configuration**.

The Port Security Configuration page displays.
6. Make sure that port security is globally enabled.

For more information, see [Configure the Global Port Security Mode](#) on page 214.
7. Select **Security > Traffic Control > Port Security > Interface Configuration**.

The Interface Configuration page displays.
8. Make sure that port security is enabled for the individual interface for which you want to view the dynamically learned MAC addresses.

For more information, see [Configure a Port Security Interface](#) on page 215.

9. Select **Security > Traffic Control > Port Security > Security MAC Address**.

10. From the **Port List** menu, select the individual interface.

The Dynamic MAC Address Table displays the MAC addresses and their associated VLANs that were learned on the selected port. The fields are described in the following table.

Field	Description
VLAN ID	The VLAN ID corresponding to the MAC address.
MAC Address	The MAC addresses learned on a specific port.

11. To convert the dynamically learned MAC address to a statically locked addresses, select the **Convert Dynamic Address to Static** check box.

12. 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.

13. To refresh the page with the latest information about the switch, click the **Update** button.

Configure Protected Ports

You can configure the ports as protected or unprotected. If a port is configured as protected, it does not forward traffic to any other protected port on the switch, but it does forward traffic to unprotected ports.

➤ 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 [Change the Default IP Address of the Switch](#) on page 9.

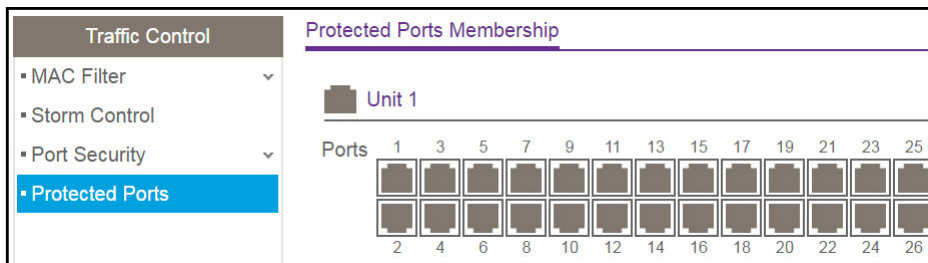
The login window opens.

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**.



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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Configure Access Control Lists

Access control lists (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 above all provide security for the network. The switch's supports IPv4 and MAC ACLs.

You can use the ACL Wizard to configure a simple ACL and apply it to selected ports (see [Use the ACL Wizard to Create a Simple ACL](#) on page 220) or you can configure an ACL manually, which allows you to set up a more complex ACL.

➤ To manually configure an ACL:

1. Create a MAC-based or IPv4-based ACL ID (see [Configure a MAC ACL](#) on page 225 or [Configure an IP ACL](#) on page 234).
2. Create a rule, assign it to a unique ACL ID, and define the rule. (see [Configure MAC ACL Rules](#) on page 227, [Configure Rules for a Basic IP ACL](#) on page 236, or [Configure Rules for an Extended IP ACL](#) on page 240).

A rule can identify protocols, source, and destination IP and MAC addresses, and other packet-matching criteria.

3. Use the ID number to assign the ACL to a port or to a LAG (see [Configure MAC Bindings](#) on page 231 or [Configure IP ACL Interface Bindings](#) on page 244).

To view ACL configuration examples, see [Access Control Lists \(ACLs\)](#) on page 294.

Use the ACL Wizard to Create a Simple ACL

The ACL Wizard helps you create a simple ACL and apply it to 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 an IP ACL](#) on page 234.

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.

Use the ACL Wizard to create an ACL

➤ **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 [Change the Default IP Address of the Switch](#) on page 9.

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 screenshot shows the 'ACL Type Selection' configuration page. On the left, there is a navigation menu with 'ACL Wizard' selected, and sub-options for 'Basic' and 'Advanced'. The main area is titled 'ACL Type Selection' and contains the following elements:

- ACL Type:** A dropdown menu set to 'ACL Based on Destination MAC'.
- ACL Based on Destination MAC:** A table with columns: Sequence Number, Action, Match Every, Destination MAC, Destination MAC Mask, and VLAN. Each column has an input field or dropdown.
- Binding Configuration:**
 - Direction:** A dropdown menu set to 'Inbound'.
 - Unit 1:** A grid of 26 ports (1-26) arranged in two rows of 13. Each port is represented by a small icon.

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 of 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.** Signifies that 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.** Signifies that 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.

ACL Based On	Fields
Destination MAC	<ul style="list-style-type: none"> • Destination MAC. Specify the destination MAC address to compare against an Ethernet frame. The valid 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 valid 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	<ul style="list-style-type: none"> • Source MAC. Specify the source MAC address to compare against an Ethernet frame. The valid 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 valid format is (xx:xx:xx:xx:xx:xx). • VLAN. Specify the VLAN ID to match within the Ethernet frame.
Destination IPv4	<ul style="list-style-type: none"> • Destination IP Address. Specify the destination IP address. • Destination IP Mask. Specify the destination IP address mask.
Source IPv4	<ul style="list-style-type: none"> • Source IP Address. Specify the source IP address. • Source IP Mask. Specify the source IP address mask.
Destination IPv4 L4 Port	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Source L4 port (protocol). Specify the source IPv4 L4 port protocol. • Source L4 port (value). Specify the source IPv4 L4 port value.

11. For this procedure (in which an ACL based on the destination MAC address is created), configure the following settings:

- a.** In the **Destination MAC** field, specify the destination MAC address that must be compared against the information in an Ethernet frame.

The valid format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC address of 01:80:C2:xx:xx:xx.

- 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 valid 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.

Valid range of values is 1 to 4093. Either a VLAN range or VLAN can be configured.

- d. In the Binding Configuration section, from the **Direction** menu, select the packet filtering direction for the ACL.

Only the inbound direction is valid.

- e. In the Ports and LAG tables in the Binding Configuration section, select the ports and LAGs to which the ACL must be applied.

- f. Click the **Add** button.

The rule is added to the ACL and is based on the destination MAC.

- 12. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 8, 10, 11, and 13 and on LAG 1. Only the Inbound option is valid. Packets that include a source address in the 192.168.3.0/16 network are forwarded by the interfaces. All other packets are dropped because every ACL includes an implicit *deny all* rule as the last rule.

The screenshot shows the ACL Wizard configuration page. It is divided into three main sections:

- ACL Type Selection:** The ACL Type is set to "ACL Based on Source IPv4".
- ACL Based on Source IPv4:** A table with the following configuration:

Sequence Number	Action	Match Every	Source IP Address	Source IP Mask
1	Permit	False	192.168.3.0	255.255.0.0
- Binding Configuration:**
 - Direction: Inbound
 - Unit 1: Ports 8, 10, 11, and 13 are selected with checkmarks.
 - LAG: LAG 1 is selected with a checkmark.

For information about the ACL Wizard, see [Use the ACL Wizard to Create a Simple ACL](#) on page 220.

Configure a 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.

The following steps are involved in defining a MAC ACL and applying it to the switch:

1. Create a MAC ACL ID (see [Configure a MAC ACL](#) on page 225).
2. Create a MAC rule (see [Configure MAC ACL Rules](#) on page 227).
3. Associate the MAC ACL with one or more interfaces (see [Configure MAC Bindings](#) on page 231).

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 233).

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 [Change the Default IP Address of the Switch](#) on page 9.

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			
Current Number of ACL	<input type="text" value="0"/>		
Maximum ACL	<input type="text" value="100"/>		
MAC ACL Table			
<input type="checkbox"/>	Name	Rules	Direction
<input type="checkbox"/>	<input type="text"/>		

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.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 rule.

7. In the **Name** field, specify the new name.

8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 rule.
7. Click the **Delete** button.

The rule 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 [Change the Default IP Address of the Switch](#) on page 9.

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 following figure does not show all columns.

Sequence Number (1 to 10)	Action	Assign Queue	Redirect Interface	Match Every	CoS	Destination MAC	Destination MAC Mask	EtherType Key
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

6. From the **ACL Name** menu, select the MAC ACL.

7. In the **Sequence Number** field, enter a whole number in the range of 1 to 10 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.

The valid range of queue IDs is 0 to 7.

10. 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.

11. 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.

12. In the **CoS** field, specify the 802.1p user priority that must be compared against the information in an Ethernet frame.

The valid range of values is 0 to 7.

13. In the **Destination MAC** field, specify the destination MAC address that must be compared against the information in an Ethernet frame.

The valid format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC address of 01:80:C2:xx:xx:xx.

14. In the **Destination MAC Mask** field, specify the destination MAC address mask that must be compared against the information in an Ethernet frame.

The valid 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.

15. From the **EtherType Key** menu, select the EtherType value that must be compared against the information in an Ethernet frame.

The valid values are as follows:

- **Appletalk**
- **ARP**
- **IBM SNA**
- **IPv4**
- **IPv6**
- **IPX**
- **MPLS multicast**
- **MPLS unicast**
- **NetBIOS**
- **Novell**
- **PPPoE**
- **Reverse ARP**
- **User Value**

16. In the **EtherType User Value** field, specify the customized EtherType value that must be used when you select **User Value** from the **EtherType Key** menu.

This value must be compared against the information in an Ethernet frame. The valid range of values is 0x0600 to 0xFFFF.

17. In the **Source MAC** field, specify the source MAC address that must be compared against the information in an Ethernet frame.

The valid format is xx:xx:xx:xx:xx:xx.

18. In the **Source MAC Mask** field, specify the source MAC address mask that must be compared against the information in an Ethernet frame.

The valid format is xx:xx:xx:xx:xx:xx.

19. In the **VLAN** field, specify the VLAN ID that must be compared against the information in an Ethernet frame.

The valid range of values is 1 to 4093. Either VLAN range or VLAN can be configured.

20. From the **Logging** menu, select whether to enable or disable logging.

When set to **Enable**, logging is enabled for this ACL rule (subject to resource availability on the switch). If the access list trap flag is also enabled, periodic traps are generated, indicating the number of times the rule was evoked during the report interval. A fixed

five-minute report interval is used for the switch. A trap is not issued if the ACL rule hit count is zero for the interval. This field is only supported for a deny action.

21. 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 [Change the Default IP Address of the Switch](#) on page 9.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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

You can assign MAC ACL lists to ACL priorities and interfaces. When an ACL is bound to an interface, all the rules that are defined are applied to the selected interface.

➤ 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 [Change the Default IP Address of the Switch](#) on page 9.

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 Configuration**.

The screenshot shows the 'MAC Binding Configuration' page. On the left is a navigation menu with 'MAC Binding Configuration' selected. The main area contains the following fields and tables:

- ACL ID:** A dropdown menu.
- Direction:** A dropdown menu set to 'Inbound'.
- Sequence Number:** A text input field containing '0', with a range '(1 to 4294967295)' indicated.
- Unit 1:** A grid of 26 ports (1-26) for binding.
- LAG:** A grid of 8 LAGs (1-8) for binding.
- Interface Binding Status:** A table with columns: Interface, Direction, ACL Type, ACL ID, Sequence Number.

- 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.

- 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 this interface and direction is used. The valid range is 1–4294967295.

- 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 and valid interfaces for ACL binding. All nonrouting physical interfaces, VLAN interfaces, and interfaces participating in LAGs are listed.

- Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the columns in the Interface Binding Status table on the page.

Table 48. Interface Binding Status table

Field	Description
Interface	The interface of the ACL assigned.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID	The ACL number (for an IP ACL) or ACL name for a MAC ACL) identifying the ACL assigned to the selected interface and direction.
Sequence Number	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.

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 [Change the Default IP Address of the Switch](#) on page 9.

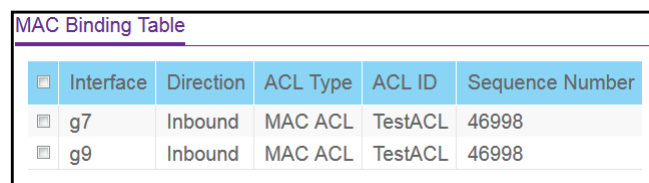
The login window opens.

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**.



<input type="checkbox"/>	Interface	Direction	ACL Type	ACL ID	Sequence Number
<input type="checkbox"/>	g7	Inbound	MAC ACL	TestACL	46998
<input type="checkbox"/>	g9	Inbound	MAC ACL	TestACL	46998

The previous figure shows examples.

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 nonconfigurable information on the page.

Table 49. MAC Binding Table

Field	Description
Interface	The interface of the ACL assigned.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID	The ACL name identifying the ACL assigned to the selected interface and direction.
Sequence Number	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.

Configure an 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.

The following steps are involved in defining an IP ACL and applying it to the switch:

1. Create an IP ACL ID (see [Configure an IP ACL](#) on page 234).
2. Create an IP rule (see [Configure Rules for a Basic IP ACL](#) on page 236 or [Configure Rules for an Extended IP ACL](#) on page 240).
3. Associate the IP ACL with one or more interfaces (see [Configure IP ACL Interface Bindings](#) on page 244).

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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

IP ACL Configuration		
Current Number of ACL	2	
Maximum ACL	100	
IP ACL Table		
IP ACL ID	Rules	Type
1	0	Basic IP ACL

The previous figure shows an example.

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 IPv4 ACL 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 named IP ACL.

7. Click the **Add** button.

The IP ACL is added to the switch configuration.

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 [Change the Default IP Address of the Switch](#) on page 9.

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.

- 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 [Change the Default IP Address of the Switch](#) on page 9.

The login window opens.

- Enter the switch's password in the **Password** field.

The default password is **password**.

The System Information page displays.

- Select **Security > ACL > Advanced > IP Rules**.

IP Rules							
ACL ID	1 ▾						
Basic ACL Rule Table							
<input type="checkbox"/>	Sequence Number	Action	Logging	Assign Queue Id	Match Every	Source IP Address	Source IP Mask
<input type="checkbox"/>	1	Deny	Disable		False	10.131.6.8	255.255.255.0

The previous figure shows an example.

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.

- 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.

- Click the **Add** button.

Standard ACL Rule Configuration(1-99)			
ACL ID	1		
Sequence Number	<input type="text" value="0"/>		
Action	<input type="radio"/> Permit <input checked="" type="radio"/> Deny	Egress Queue	<input type="text" value="0-7"/>
Logging	<input checked="" type="radio"/> Disable <input type="radio"/> Enable		
Match Every	<input checked="" type="radio"/> Disable <input type="radio"/> Enable		
Src IP Address	<input type="text"/>		
Src IP Mask	<input type="text"/>		

- Specify the following match criteria for the rule:

- Sequence Number.** Enter an ACL sequence number in the range of 1 to 10 that is used to identify the rule. An IP ACL can contain up to 10 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**, you can specify the hardware egress queue identifier that is used to handle all packets matching this IP ACL rule. The range of queue IDs is 0 to 7.
- **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 the access list trap flag is also enabled, periodic traps are generated, indicating the number of times this rule was evoked during the report interval. A fixed five-minute report interval is used for the switch. A trap is not issued if the ACL rule hit count is zero for the current interval.

- **Match Every.** From the **Match Every** menu, select 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.

This field cannot be set if a mirror interface is already configured for the IP ACL rule.

- **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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 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 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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 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 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 that is 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

IP Extended Rules													
ACL ID/Name: 101													
Extended ACL Rule Table													
Sequence Number	Action	Logging	Assign Queue ID	Match Every	Protocol Type	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask	Destination L4 Port	Service Type	
1	Deny	Disable		False	4 (IP)								

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/Name** 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 100 to 199 or a name.
7. Click the **Add** button.

Extended ACL Rule Configuration(100-199)	
ACL ID/Name	101
Sequence Number	1
Action	<input type="radio"/> Permit Egress Queue <input type="text" value=""/> (0-7) <input checked="" type="radio"/> Deny <input checked="" type="radio"/> Disable <input type="radio"/> Enable
Logging	
Match Every	<input type="text" value="False"/> ▾
Protocol Type	<input type="text" value="IP"/> ▾ <input type="text" value=""/> (0 to 255)
Src	IP Address <input type="text" value=""/> <input type="text" value=""/>
Src L4	Port <input type="text" value="Other"/> ▾ <input type="text" value=""/> (0 to 65535)
Dst	IP Address <input type="text" value=""/> <input type="text" value=""/>
Dst L4	Port <input type="text" value="Other"/> ▾ <input type="text" value=""/> (0 to 65535)
Service Type	<input type="radio"/> IP DSCP <input type="text" value=""/> ▾ <input type="text" value=""/> (0-63) <input type="radio"/> IP Precedence <input type="text" value=""/> (0-7) <input type="radio"/> IP TOS <input type="text" value=""/> <input type="text" value=""/> (00-ff)

8. Configure the following match criteria for the rule:

- **Sequence Number.** Enter a whole number in the range of 1 to 10 that is used to identify the rule. An extended IP ACL can contain up to 10 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. The range of queue IDs is 0 to 7.
- **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 the access list trap flag is also enabled, periodic traps are generated, indicating the number of times this rule was evoked during the report interval. A fixed five-minute report interval is used for the switch. A trap is not issued if the ACL rule hit count is zero for the current interval.

- **Match Every.** From the **Match Every** menu, select 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**, specify 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:

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*.

The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that *none* of the bits are important. A wildcard of 0.0.0.0 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 either enter the port number yourself (from 0 to 65535) or select one of the following protocols from the menu:

- The source TCP port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **www-http**, **smtp**, **telnet**, **pop2**, **pop3**, and **bgp**.
- The source UDP port protocols are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **ftfp**.

Each of these values translates into its equivalent port number.

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*.

- **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:

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*.

The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that *none* of the bits are important. A wildcard of 0.0.0.0 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 either enter the port number yourself (from 0 to 65535) or select one of the following protocols from the menu:

- The destination TCP port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **www-http**, **smtp**, **telnet**, **pop2**, **pop3**, and **bgp**.
- The destination UDP port protocols are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **ftfp**.

Each of these values translates into its equivalent port number.

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*.

- **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 an integer 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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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 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

You can assign ACL lists to ACL priorities and interfaces. When an ACL is bound to an interface, all the rules that are defined 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 [Change the Default IP Address of the Switch](#) on page 9.

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 Binding Configuration**.

The screenshot shows the 'IP Binding Configuration' page. At the top, there are three fields: 'ACL ID' with a dropdown menu showing '1', 'Direction' with a dropdown menu showing 'Inbound', and 'Sequence Number' with a text input field containing '0' and a range '(1 to 4294967295)'. Below these fields are two sections: 'Unit 1' and 'LAG'. The 'Unit 1' section shows a grid of 26 ports, numbered 1 through 26. The 'LAG' section shows a grid of 8 LAGs, numbered 1 through 8. At the bottom of the page, there is a table titled 'Interface Binding Status' with the following columns: Interface, Direction, ACL Type, ACL ID/Name, and Sequence Number.

6. From the **ACL ID** menu, select an existing IP ACL for you which you want to add an IP ACL interface binding.

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 this interface and direction.

A low number indicates high precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If 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 this interface and direction is used. The valid range is 1–4294967295.

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 and valid interfaces for ACL binding. All nonrouting physical interfaces, VLAN interfaces, and interfaces participating in LAGs are listed.

9. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information on the page.

Table 50. IP Binding Status table

Field	Description
Interface	The selected interface.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID/Name	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.
Sequence Number	The sequence number signifying the order of specified ACL relative to other ACLs assigned to the selected interface and direction.

View or Delete IP ACL Bindings in the IP ACL Binding Table

You can view or delete the 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 *Change the Default IP Address of the Switch* on page 9.

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					
<input type="checkbox"/>	Interface	Direction	ACL Type	ACL ID/Name	Sequence Number
<input type="checkbox"/>	g20	Inbound	IP ACL	1	51
<input type="checkbox"/>	g22	Inbound	IP ACL	1	51

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 fields in the IP ACL Binding Table on the page.

Table 51. IP ACL Binding Table

Field	Description
Interface	The interface.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID/Name	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.
Sequence Number	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.

6. Monitor the System

6

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

You can display information about the amount and type of traffic that is transmitted from and received by the switch.

This section contains the following subsections:

- [View Switch Statistics](#) on page 249
- [View Port Statistics](#) on page 252
- [View Detailed Port Statistics](#) on page 254
- [View EAP Statistics](#) on page 260
- [Perform a Cable Test](#) on page 262

View Switch Statistics

You can display detailed statistical information about the traffic the switch handles.

➤ **To view and 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 [Change the Default IP Address of the Switch](#) on page 9.

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. To view the switch statistics, select **Monitoring > Ports > Switch Statistics**.

Statistics	
ifindex	27
Octets Received	7432878
Packets Received Without Error	38599
Unicast Packets Received	1714
Multicast Packets Received	26596
Broadcast Packets Received	10289
Receive Packets Discarded	0
Octets Transmitted	2714979
Packets Transmitted Without Errors	10493
Unicast Packets Transmitted	2598
Multicast Packets Transmitted	7882
Broadcast Packets Transmitted	13
Transmit Packets Discarded	0
Most Address Entries Ever Used	12
Address Entries in Use	11
Maximum VLAN Entries	64
Most VLAN Entries Ever Used	1
Static VLAN Entries	4294967294
VLAN Deletes	0
Time Since Counters Last Cleared	0 day 4 hr 6 min 34 sec

6. Click the **Update** 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 on the page.

Table 52. Switch statistics

Field	Description
ifIndex	The interface index of the interface table entry associated with the processor of this switch.
Octets Received	The total number of octets of data received by the processor (excluding framing bits, but including FCS octets).
Packets Received Without Errors	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. This does not include multicast packets.

Table 52. Switch statistics (continued)

Field	Description
Receive Packets Discarded	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.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted Without Errors	The total number of packets transmitted out of the interface.
Unicast Packets Transmitted	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.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	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.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that were learned by this switch since the most recent reboot.
Address Entries in Use	The number of learned and static entries in the Forwarding Database Address Table for this switch.
Maximum VLAN Entries	The maximum number of VLANs allowed on this switch.
Most VLAN Entries Ever Used	The largest number of VLANs that were active on this switch since the last reboot.
Static VLAN Entries	The number of active VLAN entries on this switch that were created statically.
VLAN Deletes	The number of VLANs on this switch that were created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

View Port Statistics

You can display 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Status								
1 LAG All		Go To Interface <input type="text"/> <input type="button" value="Go"/>						
<input type="checkbox"/>	Interface	Total Packets received without Errors	Packets received with Errors	Broadcast Packets received	Packets transmitted without Errors	Transmit Packet Errors	Collision Frames	Time since counters last cleared
<input type="checkbox"/>	g1	0	0	0	0	0	0	0 day 4 hr 9 min 52 sec
<input type="checkbox"/>	g2	39045	0	10428	10616	0	0	0 day 4 hr 9 min 52 sec
<input type="checkbox"/>	g3	0	0	0	0	0	0	0 day 4 hr 9 min 52 sec
<input type="checkbox"/>	g4	0	0	0	0	0	0	0 day 4 hr 9 min 52 sec
<input type="checkbox"/>	g5	0	0	0	0	0	0	0 day 4 hr 9 min 52 sec
<input type="checkbox"/>	g6	0	0	0	0	0	0	0 day 4 hr 9 min 52 sec
<input type="checkbox"/>	g7	0	0	0	0	0	0	0 day 4 hr 9 min 52 sec
<input type="checkbox"/>	g8	0	0	0	0	0	0	0 day 4 hr 9 min 52 sec
<input type="checkbox"/>	g9	0	0	0	0	0	0	0 day 4 hr 9 min 52 sec
<input type="checkbox"/>	g10	0	0	0	0	0	0	0 day 4 hr 9 min 52 sec
<input type="checkbox"/>	g11	0	0	0	0	0	0	0 day 4 hr 9 min 52 sec

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.

To locate an interface quickly, type the interface number using the respective naming convention (for example, g1 or l1) in the **Go To Interface** field above or below the table and click the **Go** button. See [Interface Naming Conventions](#) on page 21 for more information. The entry corresponding to the specified interface is selected.

The following table describes the per-port statistics on the page.

Table 53. Port statistics

Field	Description
Interface	This object indicates the interface of the interface table entry associated with this port on an adapter.
Total Packets Received Without Errors	The total number of packets received that were without errors.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. This does not include multicast packets.
Packets Transmitted Without Errors	The number of frames that were transmitted by this port to its segment.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Collision Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time in days, hours, minutes, and seconds since the statistics for this port were last cleared.

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 [Change the Default IP Address of the Switch](#) on page 9.

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.

Reset Counters for a Specific Interface

➤ To reset the counters for a specific 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 [Change the Default IP Address of the Switch](#) on page 9.

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 next to the interface for which you want to clear the counters.

You can also type the interface number using the respective naming convention (for example, g1 or l1) in the **Go To Interface** field above or below the table and click the **Go** button. See [Interface Naming Conventions](#) on page 21 for more information. The entry corresponding to the specified interface is selected.

7. Click the **Clear** button.

The counters for the interface are reset.

View Detailed Port Statistics

You can display a variety of per-port traffic statistics.

➤ To view detailed port statistics and clear the 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 [Change the Default IP Address of the Switch](#) on page 9.

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 following figure does not show all fields on the Port Detailed Statistics page.

Port Detailed Statistics	
Interface	g1
MST ID	
ifIndex	1
Port Type	Normal
Port Channel ID	Disable
Port Role	Disabled
STP Mode	Enable
STP State	Disabled
Admin Mode	Enable
Flow Control Mode	Disable
LACP Mode	Disable
Physical Mode	Auto
Physical Status	
Link Status	Link Down
Link Trap	Enable
Packets RX and TX 64 Octets	0
Packets RX and TX 65-127 Octets	0

6. From the **Interface** menu, select the interface with the statistics to view.
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 **Update** button.
9. To clear all the counters, click the **Clear** button. This resets all statistics for this port to the default values.

The following table describes the detailed port information displayed on the page. To view information about a different port, select the port number from the **Interface** menu.

Table 54. Detailed port statistics

Field	Description
ifIndex	This object indicates the ifIndex of the interface table entry associated with this port on an adapter.
Port Type	For normal ports this field displays Normal. Otherwise, the possible values are as follows: <ul style="list-style-type: none"> • Mirrored. This port is a participating in port mirroring as a mirrored port. Look at the Port Mirroring pages for more information. • Probe. This port is a participating in port mirroring as the probe port. Look at the Port Mirroring pages for more information. • Trunk Member. The port is a member of a link aggregation trunk. Look at the Port Channel pages for more information.

Table 54. Detailed port statistics (continued)

Field	Description
Port Channel ID	If the port is a member of a port channel, the port channel's interface ID and name are shown. Otherwise, Disable is shown.
Port Role	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.
STP Mode	The Spanning Tree Protocol administrative mode associated with the port or port channel. The possible values are as follows: <ul style="list-style-type: none"> • Enable. Spanning tree is enabled for this port. • Disable. Spanning tree is disabled for this port.
STP State	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: <ul style="list-style-type: none"> • Disabled • Blocking • Listening • Learning • Forwarding • Broken
Admin Mode	The port control administration state. The port must be enabled for it to be allowed into the network. The default is Enabled.
Flow Control Mode	Indicates whether flow control is enabled or disabled for the port. This field is not valid for LAG interfaces.
LACP Mode	Indicates the Link Aggregation Control Protocol administrative state. The mode must be enabled for the port to participate in link aggregation.
Physical Mode	Indicates the port speed and duplex mode. In autonegotiation mode the duplex mode and speed are set from the autonegotiation process.
Physical Status	Indicates the port speed and duplex mode.
Link Status	Indicates whether the link is up or down.
Link Trap	Indicates whether the port sends a trap when link status changes.
Packets RX and TX 64 Octets	The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
Packets RX and TX 65-127 Octets	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).
Packets RX and TX 128-255 Octets	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).

Table 54. Detailed port statistics (continued)

Field	Description
Packets RX and TX 256-511 Octets	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).
Packets RX and TX 512-1023 Octets	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).
Packets RX and TX 1024-1518 Octets	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).
Packets RX and TX > 1518 Octets	The total number of packets (including bad packets) received or transmitted that were larger than 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Octets Received	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects must be sampled before and after a common interval.
Packets Received 64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Packets Received 65-127 Octets	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).
Packets Received 128-255 Octets	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).
Packets Received 256-511 Octets	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).
Packets Received 512-1023 Octets	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).
Packets Received 1024-1518 Octets	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).
Packets Received > 1518 Octets	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Total Packets Received Without Errors	The total number of packets received that were without errors.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.

Table 54. Detailed port statistics (continued)

Field	Description
Multicast Packets Received	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.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. This does not include multicast packets.
Receive Packets Discarded	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.
Total Packets Received with MAC Errors	The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Jabbers Received	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.
Fragments Received	The total number of packets received that were less than 64 octets in length with ERROR CRC (excluding framing bits but including FCS octets).
Undersize Received	The total number of packets received that were less than 64 octets in length with GOOD CRC (excluding framing bits but including FCS octets).
Alignment Errors	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.
Rx FCS Errors	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.
Overruns	The total number of frames discarded because this port was overloaded with incoming packets, and could not keep up with the inflow.
802.3x Pause Frames Received	A count of MAC control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
Unacceptable Frame Type	The number of frames discarded from this port due to being an unacceptable frame type.
Total Packets Transmitted (Octets)	The total number of octets of data (including those in bad packets) transmitted on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects must be sampled before and after a common interval.
Packets Transmitted 64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

Table 54. Detailed port statistics (continued)

Field	Description
Packets Transmitted 65-127 Octets	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).
Packets Transmitted 128-255 Octets	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).
Packets Transmitted 256-511 Octets	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).
Packets Transmitted 512-1023 Octets	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).
Packets Transmitted 1024-1518 Octets	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).
Packets Transmitted > 1518 Octets	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.
Maximum Frame Size	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.
Total Packets Transmitted Successfully	The number of frames that were transmitted by this port to its segment.
Unicast Packets Transmitted	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.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	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.
Total Transmit Errors	The sum of single, multiple, and excessive collisions.
Total Transmit Packets Discarded	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.

Table 54. Detailed port statistics (continued)

Field	Description
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Excessive Collision Frames	A count of frames for which transmission on a particular interface fails due to excessive collisions.
STP BPDUs Received	Number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	Number of STP BPDUs transmitted from the selected port.
RSTP BPDUs Received	Number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	Number of RSTP BPDUs transmitted from the selected port.
MSTP BPDUs Received	Number of MSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	Number of MSTP BPDUs transmitted from the selected port.
802.3x Pause Frames Transmitted	A count of MAC control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
EAPOL Frames Received	The number of valid EAPoL frames of any type that were received by this authenticator.
EAPOL Frames Transmitted	The number of EAPoL frames of any type that were transmitted by this authenticator.
Time Since Counters Last Cleared	The elapsed time in days, hours, minutes, and seconds since the statistics for this port were last cleared.

View EAP Statistics

You can display information about the incoming EAP packets.

➤ **To view EAP statistics and clear the 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 *Change the Default IP Address of the Switch* on page 9.

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**.

EAP Statistics													
GO TO INTERFACE <input type="text"/> <input type="button" value="Go"/>													
Ports	EAPoL							EAP					
	Frames Received	Frames Transmitted	Start Frames Received	Logoff Frames Received	Last Frame Version	Last Frame Source	Invalid Frames Received	Length Error Frames Received	Response/ID Frames Received	Response Frames Received	Request/ID Frames Transmitted	Request Frames Transmitted	
<input type="checkbox"/> g1	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	
<input type="checkbox"/> g2	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	
<input type="checkbox"/> g3	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	
<input type="checkbox"/> g4	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	
<input type="checkbox"/> g5	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	
<input type="checkbox"/> g6	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	
<input type="checkbox"/> g7	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	
<input type="checkbox"/> g8	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	
<input type="checkbox"/> g9	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	
<input type="checkbox"/> g10	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	
<input type="checkbox"/> g11	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	
<input type="checkbox"/> g12	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	
<input type="checkbox"/> g13	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	
<input type="checkbox"/> g14	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	

- 6. To refresh the page with the latest information about the switch, click the **Update** button.
- 7. To clear the counters for a specific port, select the check box associated with the port and click the **Clear** button.
- 8. To clear all the EAP counters for all ports on the switch, select the check box in the row heading and click the **Clear** button.

Clicking the button resets all statistics for all ports to default values.

The following table describes the EAP statistics on the page.

Table 55. EAP statistics

Field	Description
Port	Selects the port to be displayed. When the selection is changed, a page update occurs causing all fields to be updated for the newly selected port. All physical interfaces are valid.
EAPoL Frames Received	This displays the number of valid EAPoL frames of any type that were received by this authenticator.
EAPoL Frames Transmitted	This displays the number of EAPoL frames of any type that were transmitted by this authenticator.
EAPoL Start Frames Received	This displays the number of EAPoL start frames that were received by this authenticator.
EAPoL Logoff Frames Received	This displays the number of EAPoL logoff frames that were received by this authenticator.
EAPoL Last Frame Version	This displays the protocol version number carried in the most recently received EAPoL frame.
EAPoL Last Frame Source	This displays the source MAC address carried in the most recently received EAPoL frame.
EAPoL Invalid Frames Received	This displays the number of EAPoL frames that were received by this authenticator in which the frame type is not recognized.

Table 55. EAP statistics

Field	Description
EAPOL Length Error Frames Received	This displays the number of EAPoL frames that were received by this authenticator in which the frame type is not recognized.
EAP Response/ID Frames Received	This displays the number of EAP response/identity frames that were received by this authenticator.
EAP Response Frames Received	This displays the number of valid EAP response frames (other than resp/ID frames) that were received by this authenticator.
EAP Request/ID Frames Transmitted	This displays the number of EAP request/identity frames that were transmitted by this authenticator.
EAP Request Frames Transmitted	This displays the number of EAP request frames (other than request/identity frames) that were transmitted by this authenticator.

Perform a Cable Test

You can display 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

The screenshot shows the 'Cable Test' page in a web browser. At the top, there is a 'Go To Port' input field with the number '1' and a 'Go' button. Below this is a table with the following columns: 'Port', 'Cable Status', 'Cable Length', and 'Failure Location'. The table lists ports g1 through g9, all of which are currently 'Untested'.

Port	Cable Status	Cable Length	Failure Location
g1	Untested		
g2	Untested		
g3	Untested		
g4	Untested		
g5	Untested		
g6	Untested		
g7	Untested		
g8	Untested		
g9	Untested		

6. Select the check boxes that are associated with the physical ports for which you want to test the cables.
7. 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 on the page.

Table 56. Cable Test information

Field	Description
Cable Status	Displays the cable status: <ul style="list-style-type: none"> • Normal. The cable is working correctly. • Open. The cable is disconnected or a faulty connector exists. • Short. An electrical short exists in the cable. • Cable Test Failed. The cable status could not be determined. The cable might in fact be working. • Untested. The cable is not yet tested. • Invalid cable type. The cable type is unsupported. • No cable. The cable is not present.
Cable Length	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.
Failure Location	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.

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

You can set the administrative status and behavior of logs in the system buffer. The memory log stores messages in memory based upon the settings for message component and severity. These log messages are cleared when the switch reboots.

For the message log, only the latest 64 entries are displayed on the page.

➤ **To configure the memory 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 [Change the Default IP Address of the Switch](#) on page 9.

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. Next to Admin Status, select one of the following radio buttons:

- **Enable**. Enable system logging.
- **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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 64 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> Jan 01 01:25:47 172.16.166.215-1 HST [75]: weblogin.c(295)
7 %% HTTP Session 1 Login success from 172.16.166.231
```

The number contained in the angle brackets represents the message priority, which is derived from the following values:

Priority = severity level + 8.

The facility value is usually 1, which means it is a user-level message. Therefore, to determine the severity level of the message, add 8 to the severity level. 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 267.

The message was generated on Jan 01 01:25:47. The component that generated the message is HST, and it came from line 295 of file weblogin.c. This is the 7th message logged with system IP 172.16.166.215 and task-ID 1. The message indicates that the administrator logged on to the HTTP management interface from a host with an IP address of 172.16.166.231.

10. To refresh the page with the latest information about the switch, click the **Update** button.
11. To clear the messages from the buffered log in the memory, click the **Clear** button.

Message Log Format

This topic applies to the format of all logged messages that are displayed for the message log, persistent log, or console log.

Messages logged to a collector or relay through syslog use an identical format:

```
<14> Jan 01 01:25:47 172.16.166.215-1 HST [75]: weblogin.c(295) 7 %%
HTTP Session 1 Login success from 172.16.166.231
```

The example indicates a message with severity 6 (info) on the switch and is generated by component HST running in thread ID 75 on Jan 01 01:25:47 by line 295 of file weblogin.c. This is the 7th message logged with system IP 172.16.166.215 and task-ID 1.

Manage the Flash Log

The flash log is a persistent log, that is, 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 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 [Change the Default IP Address of the Switch](#) on page 9.

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. Next to Admin Status, select one of the following options:

- **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 sessions 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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The Total Number of Messages field shows the total number of persistent log messages that are stored on the switch. The maximum number of persistent log messages that can be displayed on the switch is 256.

```
00002 : <14> Jan 01 00:01:38 172.16.166.215-1 DHCP [75]:
dhcintf.c(1364) 5 %% DHCP gets IP address: 172.16.166.215
```

The previous log message example indicates a user-level message (1) with severity 6 (info) on the switch. The message is generated by component DHCP running in thread ID 75 on Jan 01 00:01:38 by line 1364 of file dhcintf.c. This is the 5th message logged.

Messages logged to a collector or relay via syslog support an identical format as the previous log message example.

Manage the Server Log

You can allow the switch to send log messages to remote logging hosts, if you configured any.

Configure the Local Log Server

➤ **To configure local log 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 *Change the Default IP Address of the Switch* on page 9.

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 page displays.

6. Next to Admin Status, select one of the following:

- **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.

8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The Server Log Configuration section displays the following information:

- The Messages Relayed field shows the number of messages forwarded by the syslog function to a syslog host. Messages forwarded to multiple hosts are counted once for each host.
- The Messages Ignored field shows the number of messages that were ignored.

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 [Change the Default IP Address of the Switch](#) on page 9.

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. Specify the following settings:

- **IP Address Type.** Specify the IP address type of the host, which can be **IPv4**, **IPv6**, 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 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 [Change the Default IP Address of the Switch](#) on page 9.

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. Select the check box that is associated with the host.
7. Change the information as needed.
8. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

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 [Change the Default IP Address of the Switch](#) on page 9.

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. Select the check box that is associated with the host.

7. Click the **Delete** button.

The host is removed.

View the Trap Logs

You can view information about the SNMP traps generated on the switch. The information can be retrieved as a file.

You can also view information about the traps that were sent.

➤ **View the trap logs and clear 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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Trap Logs**.

Trap Logs		
Number of Traps Since Last Reset		3
Trap Log Capacity		256
Number of Traps Since Log Last Viewed		0
Trap Logs		
Log	System Up Time	Trap
0	0 days 00:00:59	Cold Start: Unit: 0
1	0 days 00:00:47	Spanning Tree Topology Change: 1, Unit: 1
2	0 days 00:00:17	Link Up: g2

6. To clear all counters, click the **Clear** button.

All statistics for the trap logs are reset to their default values.

The following table describes the nonconfigurable information on the page.

Table 57. Trap Logs information

Field	Description
Number of Traps Since Last Reset	The number of traps that occurred since the switch last rebooted.
Trap Log Capacity	The maximum number of traps stored in the log. If the number of traps exceeds the capacity, the entries overwrite the oldest entries.
Number of Traps since log last viewed	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.
Log	The sequence number of this trap.

Table 57. Trap Logs information (continued)

Field	Description
System Up Time	The time when this trap occurred, expressed in days, hours, minutes, and seconds, since the last reboot of the switch.
Trap	Information identifying the trap.

Configure Port Mirroring

Port mirroring selects the network traffic for analysis by a network analyzer. This is done for specific ports of the switch. As such, many switch ports are configured as source ports and one switch port is configured as a destination port. You can configure how traffic is mirrored on a source port. Packets that are received on the source port, that are transmitted on a port, or are both received and transmitted can be mirrored to the destination port.

The packet that is copied to the destination port is in the same format as the original packet on the wire. This means that if the mirror is copying a received packet, the copied packet is VLAN tagged or untagged as it was received on the source port. If the mirror is copying a transmitted packet, the copied packet is VLAN tagged or untagged as it is being transmitted on the source port.

➤ **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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

Global Configuration

Admin Mode True False

Destination Port

Source Interface Configuration

1 LAG CPU All Go To Interface

Interface	Direction	Status
<input type="checkbox"/> g1	None	
<input type="checkbox"/> g2	None	
<input type="checkbox"/> g3	None	
<input type="checkbox"/> g4	None	
<input type="checkbox"/> g5	None	

6. Select an Admin Mode radio button:
 - **True.** Port mirroring is enabled.
 - **False.** Port mirroring is disabled.
7. From the **Destination Port** menu, select the destination port to which port traffic must be copied.

You can configure only one destination port on the switch. 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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following steps must be performed in the Source Interface Configuration section.

9. Use one of the following methods to narrow down the ports that are displayed:
 - Click the **1** link to display the physical ports of the selected unit.
 - Click the **LAG** link to display a list of LAGs only.
 - Click the **CPU** link to display a list of CPUs only.
 - Click the **All** link to display a list of all physical ports, LAGs, CPUs, and VLANs.
10. Use one of the following methods to select one or more source ports:
 - Select a specific interface by specifying the interface number using the respective naming convention (for example, g1 or l1) in the **Go To Interface** field and clicking the **Go** button. See [Interface Naming Conventions](#) on page 21 for more information. The entry corresponding to the specified interface is selected.
 - Select one or more check boxes in the Interface column.

Traffic from the selected ports is sent to the probe port.

11. From the **Direction** menu, specify the direction of the traffic that must be mirrored from the selected source ports:
 - **None.** The value is not configured. This is the default setting.

- **Tx and Rx.** Monitors transmitted and received packets.
- **Rx.** Monitors received (ingress) packets only.
- **Tx.** Monitors transmitted (egress) packets only.

12. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The Status field indicates the interface status.

7 Maintenance

7

This chapter contains the following sections:

- *Reboot the Switch*
- *Reset the Switch to Its Factory Default Settings*
- *Upload a File From the Switch*
- *Download a File to the Switch*
- *Manage Files*
- *Perform Troubleshooting*

Reboot the Switch

You can reboot the switch from the web management 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 [Change the Default IP Address of the Switch](#) on page 9.

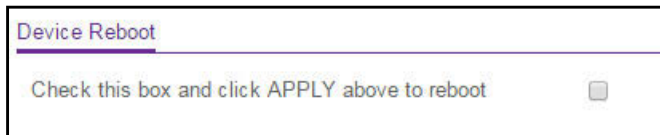
The login window opens.

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**.



Device Reboot

Check this box and click APPLY above to reboot

6. Select the check box.
7. Click the **Apply** button.

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, see [Change the Default IP Address of the Switch](#) on page 9.

➤ **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 [Change the Default IP Address of the Switch](#) on page 9.


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**.



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.

Upload a File From the Switch

You can upload configuration (ASCII), log (ASCII), and image (binary) files from the switch to the TFTP server. The switch supports system file uploads from the switch to a remote system by using either TFTP or HTTP.

Upload a File to the TFTP Server

You can upload configuration (ASCII), log (ASCII), and image (binary) files from the switch to a TFTP server on the network.

➤ **To upload a file from the switch to the 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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Upload > TFTP File Upload**.

Upload	TFTP File Upload
<ul style="list-style-type: none"> • TFTP File Upload • HTTP File Upload 	<p>File Type Text Configuration ▾</p> <p>Server Address Type IPv4 ▾</p> <p>Server Address <input type="text" value="0.0.0.0"/></p> <p>Transfer File Path <input type="text"/></p> <p>Transfer File Name <input type="text"/></p> <p>Start File Transfer <input type="checkbox"/></p>

6. From the **File Type** menu, select the type of file:
 - **Archive**. The archive is the system software image, which is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy, while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the nonactive image. This is a safety feature for faults occurring during the boot upgrade process. The default setting is Archive.
 - **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.
 - **Error Log**. The system error (persistent) log, also referred to as the event log.
 - **Trap Log**. The trap log with the system trap records.
 - **Buffered Log**. The system buffered (in-memory) log.
7. If the selection from the **File Type** menu is **Archive**, the **Image Name** menu is displayed and you must select the software image on the switch that must be uploaded to the TFTP server:
 - **image1**. Select image1 to upload image1.
 - **image2**. Select image2 to upload image2.
8. 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.

9. 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.

10. 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.

11. 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. For an archive transfer, use a `.stk` file extension.

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

13. 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 (or if it fails).

Upload a File Using HTTP

You can upload files of various types from the switch to the management system through an HTTP session by using your web browser.

➤ To upload a file from the switch to another system 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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Upload > HTTP File Upload**.

Upload	HTTP File Upload	
• TFTP File Upload	File Type	Archive
• HTTP File Upload	Image Name	image1

6. From the **File Type** menu, select the type of file:
 - **Archive.** The archive is the system software image, which is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy, while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the nonactive image. This is a safety feature for faults occurring during the boot upgrade process. The default setting is Archive.
 - **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 **Archive**, the **Image Name** menu is displayed and you must select the software image on the switch that must be uploaded to the other system:
 - **image1.** Select image1 to upload image1.
 - **image2.** Select image2 to upload image2.
8. 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 (or if it fails).

Download a File to the Switch

The switch supports system file downloads from a remote system to the switch by using either TFTP or HTTP.

Download a File to the Switch Using TFTP

You can download device software, the image file, and the configuration 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 [Download a File to the Switch Using HTTP](#) on page 282 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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Download > TFTP File Download**.

6. From the **File Type** menu, select the type of file:
 - **Archive.** The archive is the system software image, which is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy, while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the nonactive image. This is a safety feature for faults occurring during the boot upgrade process. The default setting is Archive.
 - **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 **Archive**, 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 (or if it fails).

Download a File to the Switch Using HTTP

You can download files of various types to the switch through an HTTP session by using your 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.

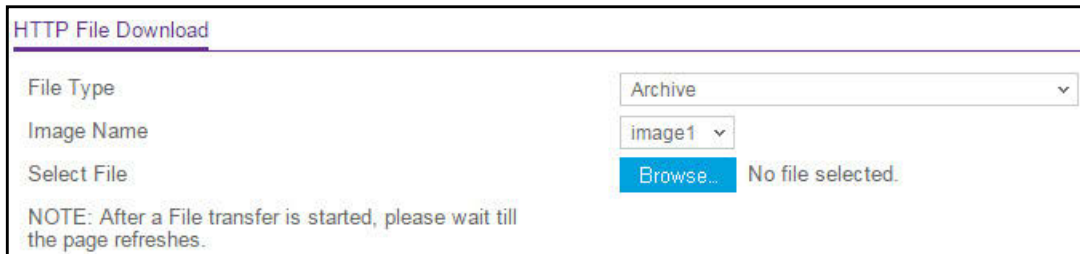
If you do not know the IP address of the switch, see *Change the Default IP Address of the Switch* on page 9.

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 > Download > HTTP File Download**.



HTTP File Download

File Type: Archive

Image Name: image1

Select File: No file selected.

NOTE: After a File transfer is started, please wait till the page refreshes.

6. From the **File Type** menu, select the type of file:

- **Archive.** 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. The default setting is Archive.
- **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 **Archive**, 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. Next to Select File, click the **Browse** button and locate 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. The page refreshes automatically when the file transfer completes (or if it fails).

Note: 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 text configuration file is downloaded, the switch applies the configuration automatically.

Manage Files

The system 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 during subsequent switch restarts. This feature reduces switch down time when you are upgrading or downgrading the switch software.

A legacy software version can ignore (that is, might not load) a configuration file that is created by a newer software version. When a configuration file created by the newer software version is discovered by the system running an older version of the software, the system displays an appropriate warning.

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 during the next boot cycle, configure an image description, or delete an image. This feature reduces switch down time when you are upgrading or downgrading the software image.

➤ 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 [Change the Default IP Address of the Switch](#) on page 9.

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**.

File Management	Dual Image Configuration
• Dual Image ^	Image Name <input type="text" value="image1"/>
• Dual Image Configuration	Current-active <input type="text" value="image1"/>
• Dual Image Status	Image Description <input type="text" value=""/> (0 to 127)
	Activate Image <input type="checkbox"/>
	Delete Image <input type="checkbox"/>

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.

7. To specify a name for the selected image, enter one in the **Image Description** field.
8. Select the **Activate Image** check box.
9. Click the **Apply** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

Note: After activating an image, you must perform a system reset of the switch to run the new code. The switch continues running the image shown in the Current-active field until the switch reboots.

Delete an Image

➤ To delete an 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 [Change the Default IP Address of the Switch](#) on page 9.
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.

- 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.

- Select the **Delete** Image check box.
- Click the **Apply** button.

The image is removed.

Display the Dual Image Status

You can display information about the active and backup images on the switch.

➤ To display the dual image status:

- 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.

- Launch a web browser.
- 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 [Change the Default IP Address of the Switch](#) on page 9.

The login window opens.

- Enter the switch's password in the **Password** field.

The default password is **password**.

The System Information page displays.

- Select **Maintenance > File Management > Dual Image > Dual Image Status**.

The following table describes the nonconfigurable information on the page.

Table 58. Dual Image Status information

Field	Description
Image1 Ver	The version of the image1 code file.
Image2 Ver	The version of the image2 code file.
Current-active	The currently active image on this switch.
Next-active	The image to be used on the next restart of this switch.
Image1 Description	The description associated with the image1 code file.
Image2 Description	The description associated with the image2 code file.

Perform Troubleshooting

You can send a ping and perform a memory dump.

Ping an IPv4 Address

You can specify that the switch must send a ping request to a specified IP address. You can use this to check whether the switch can communicate with a particular IP station. When you click the **Apply** button, the switch sends a specified number of ping requests and the results are displayed.

If a reply to the ping is not received, the following message displays:

```
Tx = Count, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec
```

If a reply to the ping is received, the following message displays:

```
Reply From a.b.c.d: icmp_seq = 0. time= xyz usec.
Reply From a.b.c.d: icmp_seq = 1. time= abc usec.
Reply From a.b.c.d: icmp_seq = 2. time= def usec.
Tx = count, Rx = count Min/Max/Avg RTT = xyz/abc/def msec
```

➤ To configure the settings and ping a host on the network:

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 [Change the Default IP Address of the Switch](#) on page 9.

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 > Ping IPv4**.

6. In the **IP Address/Host Name** field, enter the IP address or host name of the device that must be pinged.
7. In the **Count** field, enter the number of echo requests that must be sent.
The default is 3. The range is 1 to 15.
8. In the **Interval** field, enter the time between ping packets in seconds.
The default is 3 seconds. The range is 1 to 60.
9. In the **Size** field, enter the size of the ping packet. The default is 0 bytes. The range is 0 to 1518.
10. Click the **Apply** button.
The specified address is pinged. The results are displayed below the configurable data in the Results field.

Ping an IPv6 Address

You can send a ping request to a specified host name or IPv6 address. You can use this to check whether the switch can communicate with a particular IPv6 station. When you click the **Apply** button, the switch sends a specified number of ping requests and the results are displayed below the configurable data. The output displays the following:

```
Send count=n, Receive count=n from (IPv6 Address). Average round trip
time = n ms.
```

➤ To send an IPv6 ping:

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 [Change the Default IP Address of the Switch](#) on page 9.
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 > Ping IPv6**.

6. In the **IPv6 Address/Hostname** field, enter the IPv6 address or host name of the station that must be pinged.

The format is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. The maximum number of characters is 255.

7. In the **Count** field, enter the number of echo requests that must be sent.

The range is 1 to 15. The default is 3.

8. In the **Interval** field, enter the time in seconds between ping packets.

The range is 1 to 60. The default is 3.

9. In the **Datagram Size** field, enter the datagram size.

The valid range is 0 to 13000. The default is 0 bytes.

10. Click the **Apply** button.

The specified address is pinged. The results are displayed below the configurable data in the Results field.

Enable and Perform Remote Diagnostics

You can enable or disable the option to access the switch remotely. When remote access is enabled, you can perform 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 [Change the Default IP Address of the Switch](#) on page 9.

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.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

A Configuration Examples



This appendix contains information about how to configure the following features.

The appendix contains the following sections:

- *Virtual Local Area Networks (VLANs)*
- *Access Control Lists (ACLs)*
- *Differentiated Services (DiffServ)*
- *802.1X*
- *MSTP*

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 106.
- 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.
- If the port is a member of the VLAN specified by the packet's VLAN ID, the packet can be sent to other ports with the same VLAN ID.

- Packets leaving the switch are either tagged or untagged, depending on the setting for that port's VLAN membership properties. A U for a given port means that packets leaving the switch from that port are untagged. Inversely, a T for a given port means that packets leaving the switch from that port are tagged with the VLAN ID that is associated with the port.

The example given in this section comprises numerous steps to illustrate a wide range of configurations to help provide an understanding of tagged VLANs.

VLAN 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 100), 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 103) 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 106), 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 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 MAC ACL](#) on page 225).

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 227.

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 231.)

You can assign an optional sequence number to indicate the order of this access list relative to other access lists if any are already assigned to this interface and direction.

4. The MAC Binding Table displays the interface and MAC ACL binding information. (See [View or Delete MAC ACL Bindings in the MAC Binding Table](#) on page 233.)

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 an IP ACL](#) on page 234.)
2. On the IP Rules page, create a rule for IP ACL 1 with the following settings:
 - **Sequence Number.** 1
 - **Action.** Deny
 - **Assign Queue ID.** 0 (optional: 0 is the default value)
 - **Match Every.** False
 - **Source IP Address.** 192.168.187.0
 - **Source IP Mask.** 0.0.0.255

For additional information about IP ACL rules, see [Configure Rules for a Basic IP ACL](#) on page 236.

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 244.)

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. On IP Binding Table page, view the interfaces and IP ACL binding information. (See [View or Delete IP ACL Bindings in the IP ACL Binding Table](#) on page 246)

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 or OR operations to build complex MF-classifiers (by specifying a class type of *all* or *any*, respectively). That is, within a single class, multiple match criteria are grouped together as an AND expression or a sequential OR expression, depending on the defined class type. Only classes of the same type can be nested; class nesting does not allow for the negation (*exclude* option) of the referenced class.

To configure DiffServ, you must define service levels, namely the forwarding classes/PHBs identified by a given DSCP value, on the egress interface. 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. Special treatment can be applied to out-of-profile packets that are either in excess of the conformance specification or are nonconformant. The DiffServ feature supports the following types of traffic policing treatments (actions):
 - **drop.** The packet is dropped.
 - **mark cos.** The 802.1p user priority bits are (re)marked and forwarded.
 - **mark dscp.** The packet DSCP is (re)marked and forwarded.
 - **mark prec.** The packet IP Precedence is (re)marked and forwarded.
 - **send.** The packet is forwarded without DiffServ modification.

Color Mode Awareness. Policing in the DiffServ feature uses either color blind or color aware mode. Color blind mode ignores the coloration (marking) of the incoming packet. Color aware mode takes into consideration the current packet marking when the switch determines the policing outcome. An auxiliary traffic class is used in conjunction with the policing definition to specify a value for one of the 802.1p, secondary 802.1p, IP DSCP, or IP precedence fields designating the incoming color value to be used as the conforming color. You can also specify the color of traffic that exceeds the threshold.

- **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 249.
- **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 about this page, see *Configure a DiffServ Class* on page 163.

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 about this page, see [Configure a DiffServ Class](#) on page 163.

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 about this page, see [Configure a DiffServ Policy](#) on page 168.

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.** 10000 (which means 10000*16 kb/s).
 - **Confirm Action.** Send
 - **Violate Action.** Drop

For more information about this page, see [Configure a DiffServ Policy](#) on page 168.

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 174.)

802.1X

Local area networks (LANs) are often deployed in environments that permit unauthorized devices to be physically attached to the LAN infrastructure, or permit unauthorized users to attempt to access the LAN through equipment already attached. In such environments 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:

1. **Authenticator.** A port that enforces authentication before allowing access to services available through that port.
2. **Supplicant.** A port that attempts to access services offered by the authenticator.

Additionally, there exists a third role:

3. **Authentication server.** Performs the authentication function necessary to check the credentials of the supplicant on behalf of the authenticator.

All three roles are required 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.

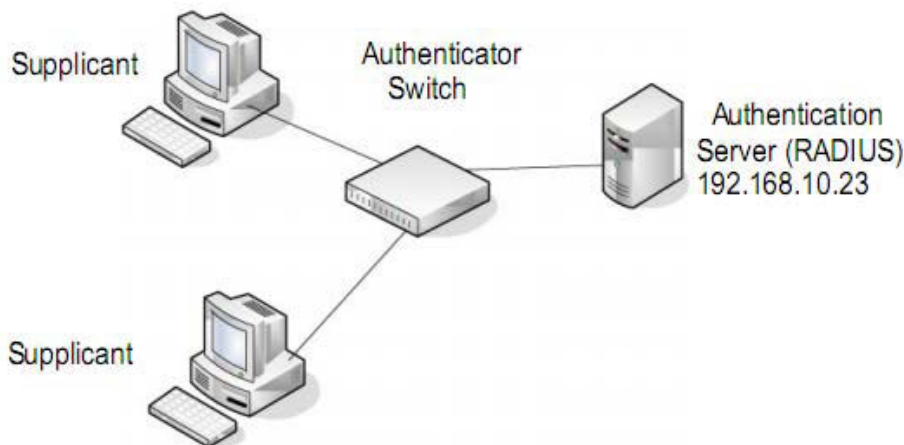


Figure 1. 802.1X authentication roles

802.1X Example Configuration

This example shows how to configure the switch so that 802.1X-based authentication is required on the ports in a corporate conference room (g5–g8). These ports are available to visitors and 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 (see [Configure 802.1X Settings for a Port](#) on page 204), select ports **g5**, **g6**, **g7**, and **g8**.
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 g5–g8, enter **150** to assign these ports to the guest VLAN.
You can configure additional settings to control access to the network through the ports. See [Configure a Port Security Interface](#) on page 215 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 214.)

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 (see [Add a Primary RADIUS Authentication Server to the Switch](#) on page 182), 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 [Configure RADIUS Servers](#) on page 180.

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 191.)

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.

MSTP

Spanning Tree Protocol (STP) runs on bridged networks to help eliminate loops. If a bridge loop occurs, the network can become flooded with traffic. IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) supports multiple instances of spanning tree to efficiently channel VLAN traffic over different interfaces. Each instance of the spanning tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree, with slight modifications in the working but not the end effect (chief among the effects is the rapid transitioning of the port to the forwarding state).

The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full-duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to the Forwarding state and the suppression of Topology Change Notification. These features are represented by the parameters `pointtopoint` and `edgeport`. MSTP is compatible to both RSTP and STP. It behaves 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 given VLAN throughout a bridged LAN comprising arbitrarily interconnected networking devices, each operating MSTP, STP, or RSTP. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) regions composed of LANs and or MSTP bridges. These regions and the other bridges and LANs are connected into a single Common Spanning Tree (CST). (IEEE DRAFT P802.1s/D13)

MSTP connects all bridges and LANs with a single Common and Internal Spanning Tree (CIST). The CIST supports the automatic determination of each MST region, choosing its maximum possible extent. The connectivity calculated for the CIST provides the CST for interconnecting these regions, and an Internal Spanning Tree (IST) within each region. MSTP

ensures that frames with a given VLAN ID are assigned to one and only one of the MSTIs or the IST within the region, that the assignment is consistent among all the networking devices in the region, and that the stable connectivity of each MSTI and IST at the boundary of the region matches that of the CST. The stable active topology of the bridged LAN with respect to frames consistently classified as belonging to any given VLAN thus simply and fully connects all LANs and networking devices throughout the network, though frames belonging to different VLANs can take different paths within any region, per IEEE DRAFT P802.1s/D13.

All bridges, whether they use STP, RSTP, or MSTP, send information in configuration messages 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 VID 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 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.

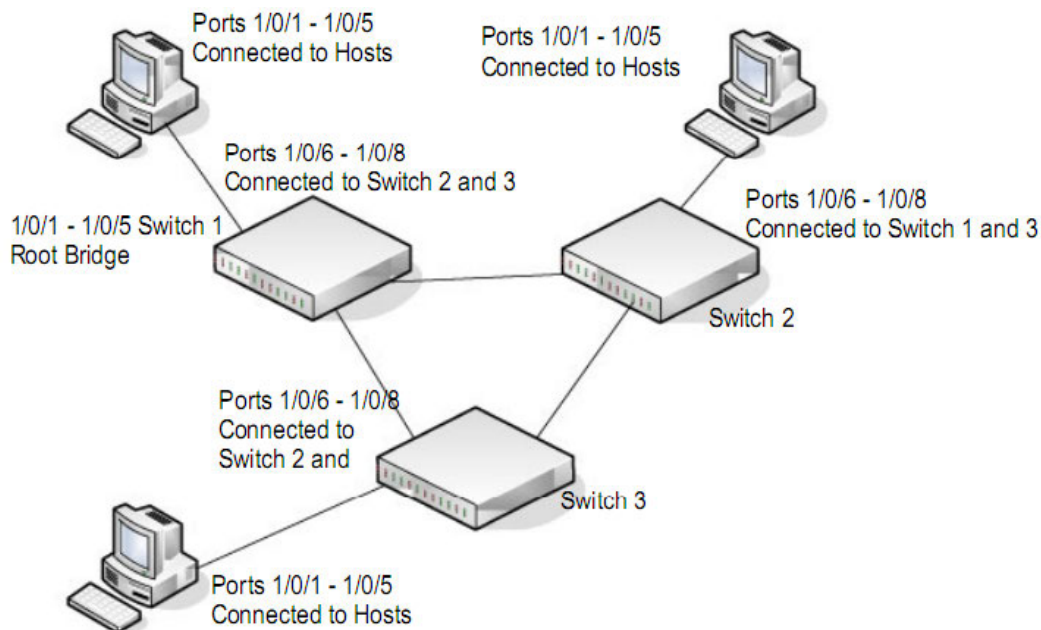


Figure 2. MSTP sample configuration

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 101).
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 101).
3. On the STP Configuration page, enable the Spanning Tree State option (see [Configure STP Settings](#) on page 117).

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 (see [Configure CST Port Settings](#) on page 121), set the bridge priority value for each of the three switch connections to force Switch 1 to be the root bridge:
 - **Connection to Switch 1.** 4096
 - **Connection to Switch 2.** 12288
 - **Connection to 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 CST Settings](#) on page 119).

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 CST Port Settings](#) on page 121).
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.

On the CST Port Status page you can view spanning tree information about each port.

9. On the MST Configuration page (see [Manage MST Settings](#) on page 125), 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 124.

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.

B Specifications and Default Settings

B

This appendix describes the default settings for the switch and for its software features.

The 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*

Switch Default Settings

The following table describes the switch default settings.

Table 59. Switch default settings

Feature	Default
IP address	192.168.0.239
Subnet mask	255.255.255.0
Default gateway	192.168.0.254
Protocol	DHCP
Management VLAN ID	1
Minimum password length	Eight characters
IPv6 management Mode	None
SNTP client	Disabled
Global logging	Enabled
RAM logging	Enabled (Severity level: debug and above)
Persistent (FLASH) logging	Disabled
DNS	Enabled (No servers configured)
SNMP Traps	Enabled
Auto Save	Enabled
RMON	Enabled
TACACS+	Not configured
RADIUS	Not configured
SSL	Disabled
Denial of service protection	Disabled
Dot1x authentication (IEEE 802.1X)	Disabled
MAC-based port security	All ports are unlocked
Access control lists (ACL)	Not configured
Protected ports	None
Line blocking prevention	Disabled
Advertised port speed	Maximum capacity
Broadcast storm control	Disabled

Table 59. Switch default settings (continued)

Feature	Default
MAC table address aging	300 seconds (dynamic addresses)
Default VLAN ID	1
Default VLAN name	Default
Voice VLAN	Disabled
Guest VLAN	Disabled
Multiple Spanning Tree	Disabled
Link aggregation	No link aggregation groups (LAGs) configured
LACP system priority	32768
DiffServ	Disabled
IGMP snooping	Disabled
IGMP snooping querier	Disabled

General Feature Default Settings

The following table describes the general feature default settings.

Table 60. General feature default settings

Feature Name/Setting	Default
Virtual LAN (IEEE 802.1Q)	
Default VLANs	1 (Default) Note: All ports are members of default VLAN
PVID	1
Acceptable Frame Types	Admit All
Ingress Filtering	Disabled
Port Priority	0
Jumbo Frames	
Maximum Frame Size	1518
Flow Control	
Admin Mode	Disabled
802.1X	
Port Based Authentication State	Disabled

Table 60. General feature default settings (continued)

Feature Name/Setting	Default
EAPOL Flood Mode	Disabled
Port Control	Auto
Guest VLAN ID	0
Guest VLAN Period	90
Periodic Reauthentication	Disabled
Reauthentication Period	3600
Quiet Period	60
Resending EAP	30
Max EAP Requests	2
Supplicant Timeout	30
Server Timeout	30
STP/RSTP/MSTP, Global	
Spanning Tree State	Enabled
STP Operation Mode	IEEE 802.1s RSTP
Configuration Name	<MAC address>
Configuration Revision Level	0
BPDU Flooding	Disabled
CST Bridge Priority	32768
CST Bridge Max Age	20
CST Bridge Hello Time	2
CST Bridge Forward Delay	15
CST Spanning Tree Max Hops	20
MST Default Instance ID	0
MST Instance 0 Priority	32768
MST Instance 0 VLAN IDs	1
STP/RSTP/MSTP, Interface	
CST STP Status	Enabled
CST Fast Link	Enabled
CST BDPUs Forwarding	Disabled

Table 60. General feature default settings (continued)

Feature Name/Setting	Default
CST Path Cost	0
CST Priority	128
Link Aggregation	
Lag Name	LAG <n> where n is 1 to 8
Admin Mode	Enabled
STP Mode	Enabled
Link Trap	Enabled
LAG Type	Static
Local Link Discovery Protocol (LLDP), Global	
TLV Advertised Interval	30
Hold Multiplier	4
Reinitializing Delay	2
Transmit Delay	5
Fast Start Duration	3
Local Link Discovery Protocol (LLDP), Interface	
Admin Status	Tx and Rx
Management IP Address	Auto Advertise
Notification	Enabled
Optional TLVs	Enabled
DHCP Snooping, Global	
Admin Mode	Disabled
MAC Address Validation	Enabled
DHCP Snooping, Interface	
Trust Mode	Disabled
Class of Service (CoS), Global	
Trust Mode	802.1p

Table 60. General feature default settings (continued)

Feature Name/Setting	Default
802.1p to Queue Mapping (802.1p -> Queue)	0 -> 1 1 -> 0 2 -> 2 3 -> 3 4 -> 4 5 -> 5 6 -> 6 7 -> 7
DSCP to Queue Mapping (DSCP -> Queue)	Class Selector: (CS 0) 000000 -> 1 (CS 1) 001000 -> 0 (CS 2) 010000 -> 2 (CS 3) 011000 -> 3 (CS 4) 100000 -> 4 (CS 5) 101000 -> 5 (CS 6) 110000 -> 6 (CS 7) 111000 -> 7 Assured Forwarding: (AF 11) 001010 -> 0 (AF 12) 001100 -> 0 (AF 13) 001110 -> 0 (AF 21) 010010 -> 0 (AF 22) 010100 -> 0 (AF 23) 010110 -> 0 (AF 31) 011010 -> 1 (AF 32) 011100 -> 1 (AF 33) 011110 -> 1 (AF 41) 100010 -> 1 (AF 42) 100100 -> 1 (AF 43) 100110 -> 1 Expedited Forwarding: (EF) 101110 -> 2 Other: (1) 000001 -> 1 (2) 000010 -> 1 (3) 000011 -> 1 (4) 000100 -> 1 (5) 000101 -> 1 (6) 000110 -> 1 (7) 000111 -> 1 (9) 001001 -> 0

Table 60. General feature default settings (continued)

Feature Name/Setting	Default
DSCP to Queue Mapping (DSCP -> Queue) (continued from previous page)	(11) 001011 -> 0 (13) 001101 -> 0 (15) 001111 -> 0 (17) 010001 -> 0 (19) 010011 -> 0 (21) 010101 -> 0 (23) 010111 -> 0 (25) 011001 -> 1 (27) 011011 -> 1 (29) 011101 -> 1 (31) 011111 -> 1
	(33) 100001 -> 2 (35) 100011 -> 2 (37) 100101 -> 2 (39) 100111 -> 2 (41) 101001 -> 2 (43) 101011 -> 2 (45) 101101 -> 2 (47) 101111 -> 2 (49) 110001 -> 3 (50) 110010 -> 3 (51) 110011 -> 3 (52) 110100 -> 3 (53) 110101 -> 3 (54) 110110 -> 3 (55) 110111 -> 3 (57) 111011 -> 3 (58) 111010 -> 3 (59) 111011 -> 3 (60) 111100 -> 3 (61) 111101 -> 3 (62) 111110 -> 3 (63) 111111 -> 3
Class of Service (CoS), Interface	
Trust Mode	802.1p
Interface Shaping Rate	0

Table 60. General feature default settings (continued)

Feature Name/Setting	Default
802.1p to Queue Mapping (802.1p → Queue)	0 -> 1 1 -> 0 2 -> 2 3 -> 3 4 -> 4 5 -> 5 6 -> 6 7 -> 7
Queue Minimum Band Width	0
Queue Scheduler Type	Weighted
Auto-VoIP, Protocol-Based	
Admin Mode	Disabled
Prioritization Type	Traffic Class
Auto-VoIP Traffic Class	7
Auto-VoIP, OUI-Based	
Admin Mode	Disabled
Auto-VoIP VLAN	0
OUI-based priority	7

System Setup and Maintenance Settings

The following table describes the system setup and maintenance settings.

Table 61. System setup and maintenance settings

Feature	Sets Supported	Default
Boot code update	1	N/A
DHCP/manual IP	1	DHCP enabled/192.168.0.239
System name configuration	1	NULL
Configuration save/restore	1	N/A
Firmware upgrade	1	N/A
Restore defaults	1 (web and front-panel button)	N/A
Dual image support	1	Enabled
Factory reset	1	N/A

Port Characteristics

The following table describes the port characteristics.

Table 62. Port characteristics

Feature	Sets Supported	Default
Energy Efficient Ethernet (EEE)	All ports	Disabled
Auto negotiating speed and full/half duplex	All ports	Auto negotiation
Auto MDI/MDIX	for cross over cables on all ports	Enabled
802.3x flow control/back pressure	1 (per system)	Disabled
Port mirroring: TX, RX, Both	1	Disabled
Port trunking (aggregation)	8	Preconfigured
802.1D spanning tree	1	Disabled
802.1w RSTP	1	Enabled
802.1s spanning tree	4 instances	Disabled
Static 802.1Q tagging	256	VID = 1 Max member ports are equal to the number of ports on the switch
Learning process	Supports static and dynamic MAC entries	Dynamic learning is enabled by default

Traffic Control Settings

The following table describes the traffic control settings.

Table 63. Traffic control settings

Feature	Sets Supported	Default
Storm control	All ports	Disabled
Jumbo frame	All ports	Disabled Max = 9216 bytes

Quality of Service Settings

The following table describes the Quality of Service settings.

Table 64. Quality of Service settings

Feature	Sets Supported	Default
Number of queues	8	N/A
802.1p	1	Enabled
DSCP	1	Disabled
Egress Rate limiting	All ports	Disabled

Security Settings

The following table describes the security settings.

Table 65. Security settings

Feature	Sets Supported	Default
802.1X	All ports	Disabled
MAC ACL	100 (shared with IP and IPv6 ACLs)	All MAC addresses allowed
IP ACL	100 (shared with MAC and IPv6 ACLs)	All IP addresses allowed
Password control access	1	Idle timeout = 5 mins. Password = password
Management security	1 profile with 20 rules for HTTP/HTTPS/SNMP access to allow/deny an IP address/subnet	All IP addresses allowed
Port MAC lock down	All ports	Disabled

System Management Settings

The following table describes the system management settings.

Table 66. System management settings

Feature	Sets Supported	Default
Multi-session web connections	4	Enabled
SNMPv1/v2 SNMPv3	Max 5 community entries	Enabled (read, read/write communities)
Time control	1 (Local or SNTP)	Local Time enabled
LLDP/LLDP-MED	All ports	Enabled
Logging	3 (Memory/Flash/Server)	Memory Log enabled
MIB support	1	Disabled
Smart Control Center	N/A	Enabled
Statistics	N/A	N/A

Settings for Other Features

The following table describes the settings for other features.

Table 67. Settings for other features

Feature	Sets Supported	Default
IGMP snooping v1/v2/v3	All ports	Disabled
Configurations upload/download	1	N/A
EAPoL flooding	All ports	Disabled
BPDU flooding	All ports	Disabled
Static multicast groups	32	None
Number of DHCP snooping bindings	256 (total number for static and dynamic bindings together)	N/A