NETGEAR®

User Manual

S350 Series 8-Port Gigabit Ethernet Smart Switch

User Manual

Models

GS308T

GS310TP

September 2021
202-11890-04

NETGEAR, Inc.
350 East Plumeria Drive
San Jose, CA 95134, USA

Support and Community

Visit netgear.com/support to get your questions answered and access the latest downloads.

You can also check out our NETGEAR Community for helpful advice at community.netgear.com.

Regulatory and Legal

Si ce produit est vendu au Canada, vous pouvez accéder à ce document en français canadien à https://www.netgear.com/support/download/.

(If this product is sold in Canada, you can access this document in Canadian French at https://www.netgear.com/support/download/.)

For regulatory compliance information including the EU Declaration of Conformity, visit https://www.netgear.com/about/regulatory/.

See the regulatory compliance document before connecting the power supply.

For NETGEAR's Privacy Policy, visit https://www.netgear.com/about/privacy-policy.

By using this device, you are agreeing to NETGEAR's Terms and Conditions at https://www.netgear.com/about/terms-and-conditions. If you do not agree, return the device to your place of purchase within your return period.

Do not use this device outdoors. For products that support Power over Ethernet (PoE), the PoE source is intended for intra building connection only.

Applicable to 6 GHz devices only: Only use the device indoors. The operation of 6 GHz devices is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet. Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

This switch is designed for indoor use only. If you want to connect to a device located outdoors, the outdoor device must be properly grounded and surge protected, and you must install an Ethernet surge protector inline between the switch and the outdoor device. Failure to do so can damage the switch.

WARNING: Before connecting this switch to outdoor cables or devices, see https://kb.netgear.com/000057103 for safety and warranty information.

Trademarks

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

Revision History

Publication Part Number	Publish Date	Comments
202-11890-04	September 2021	We removed “Managed Pro” from the product name.
202-11890-03	August 2021	We changed Access the Local Browser Interface on page 18. We changed Configure CoS Interface Settings for an Interface on page 176. We removed information about the Insight app.
202-11890-02	November 2019	We made changes to the information in and the organization of Chapter 1, Get Started and Chapter 5, Manage Device Security. We made multiple other minor changes and minor corrections in the manual. We published the manual in a new format.
202-11890-01	January 2019	First publication.

Contents

Chapter 1 Get Started

Available Publications 10
Switch Management and Discovery Overview 11
Options to Change the Default IP Address of the Switch 11
Discover or Change the Switch IP Address 12
Discover the Switch in a Network With a DHCP Server. 12
Discover the Switch in a Network Without a DHCP Server. 13
Use the NETGEAR Switch Discovery Tool to Access the Switch. 15
Configure a Static IP Address From a Directly Connected Computer . 16
About the User Interfaces 18
Software Requirements to Use the Local Browser Interface. 18
Supported Web Browsers 18
Access the Local Browser Interface 18
Navigation Tabs, Configuration Menus, and Page Menu 20
Configuration and Status Options 21
Buttons in the Local Browser Interface. 21
User-Defined Fields. 22
Change the Language of the Local Browser Interface 22
Use the Device View of the Local Browser Interface 23
Power LED in the Device View. 24
PoE Max LED in the Device View (Model GS310TP) 25
Interface Naming Conventions. 25
Configure Interface Settings 25
Context-Sensitive Help and Access to the Support WebSite 29
Access the User Guide Online 29
Register Your Product. 30

Chapter 2 Configure System Information

View and Configure the Switch Management Settings 32
View or Define System Information 32
View the System CPU Status 35
Configure the IP Network and VLAN Settings for the Local Browser Interface 37
Configure the Time Settings 39
Configure Denial of Service Settings 53
Configure DNS Settings 56
Configure Green Ethernet Settings 60
Use the Device View. 63
Configure PoE 63

Configure the Global PoE Settings 63
Configure the PoE Port Settings 64
Configure SNMP 68
Configure the SNMPv1/v2 Community 68
Configure SNMPv1/v2 Trap Settings 70
Configure SNMPv1/v2 Trap Flags 73
View the Supported MIBs 74
Configure SNMP V3 Users 75
Configure LLDP 76
Configure LLDP Global Settings 76
Configure LLDP Port Settings 78
View the LLDP-MED Network Policy 79
Configure LLDP-MED Port Settings 81
View the Local Information Advertised Through LLDP 82
View LLDP Neighbors Information 84
Configure DHCP Snooping 87
Configure the Global DHCP Snooping Settings 88
Enable DHCP for All Interfaces in a VLAN 89
Configure DHCP Snooping Interface Settings 89
Configure Static DHCP Bindings 91
Configure DHCP Snooping Persistent Settings 92
View or Clear DHCP Snooping Statistics 93
Set Up PoE Timer Schedules 94
Create a PoE Timer Schedule 95
Specify the Settings for an Absolute PoE Timer Schedule 95
Specify the Settings for a Recurring PoE Timer Schedule 97
Change the Settings for a Recurring PoE Timer Schedule Entry 99
Delete a PoE Timer Schedule Entry 100
Delete a PoE Timer Schedule 100

Chapter 3 Configure Switching

Configure the Port Settings and Maximum Frame Size 103
Configure Link Aggregation Groups 106
Configure LAG Settings 106
Configure LAG Membership 108
Set the LACP System Priority 109
Set the LACP Port Priority Settings 110
Configure VLANs 111
Configure VLAN Settings 112
Configure VLAN Membership 115
View the VLAN Status 117
Configure Port PVID Settings 118
Configure a MAC-Based VLAN 120
Configure Protocol-Based VLAN Groups 122
Configure Protocol-Based VLAN Group Membership 123
Configure a Voice VLAN 125
Configure Auto-VoIP 126

Configure Protocol-Based Port Settings for VoIP 127
Configure Auto-VoIP OUI-Based Properties 128
Configure the OUI-Based Port Settings 129
Manage the OUI Table 130
Display the Auto-VoIP Status 132
Configure Spanning Tree Protocol 133
Configure the STP Settings and View the STP Status 133
Configure and View the CST Settings 135
Configure and View the CST Port Settings 137
View the CST Port Status 139
View Rapid STP Information 141
Manage MST Settings 142
Configure and View the Port Settings for an MST Instance 144
View the STP Statistics 147
Configure Multicast 148
View and Search the MFDB Table 148
View the MFDB Statistics 149
Configure the Auto-Video Multicast Settings 150
About IGMP Snooping 151
Configure IGMP Snooping 151
Configure IGMP Snooping for Interfaces 153
View, Search, or Clear the IGMP Snooping Table 155
Configure IGMP Snooping for VLANs 156
Modify IGMP Snooping Settings for a VLAN 157
Disable IGMP Snooping on a VLAN 158
Configure a Multicast Router Interface 159
Configure a Multicast Router VLAN 160
IGMP Snooping Querier Overview 161
Configure an IGMP Snooping Querier 161
Configure an IGMP Snooping Querier for VLANs 162
Display IGMP Snooping Querier for VLAN Status 163
View, Search, and Manage the MAC Address Table 165
View, Search, or Clear the MAC Address Table 165
Set the Dynamic Address Aging Interval 167
Add a Static MAC Address to the MAC Address Table 168
Configure Layer 2 Loop Protection 169
Configure Global Layer 2 Loop Protection 169
View and Configure Layer 2 Loop Protection on a Port 170

Chapter 4 Configure Quality of Service

Quality of Service Concepts 174
Manage Class of Service 174
CoS Configuration Concepts 174
Configure Global CoS Settings 175
Configure CoS Interface Settings for an Interface 176
Configure CoS Queue Settings for an Interface 178
Map 802.1p Priorities to Queues 179
Map DSCP Values to Queues 180

Manage Differentiated Services 181
Defining DiffServ 182
Configure and Display Global DiffServ Settings. 182
Configure a DiffServ Class 184
Configure a DiffServ Policy. 190
Configure the DiffServ Service Interface 195
View DiffServ Service Statistics 197

Chapter 5 Manage Device Security

Configure the Management Security Settings 199
Change the Password for the Local Browser Interface 199
Manage the RADIUS Settings 200
Configure TACACS+ 209
Configure Authentication Lists 212
Manage the Smart Control Center Utility 216
Configure Management Access. 217
Configure HTTP Access Settings. 217
Configure HTTPS Access Settings 218
Manage Certificates for HTTPS Access 219
Transfer an Existing Certificate to the Switch 221
Manage Access Control to the Switch 224
Configure Port Authentication 230
Configure Global 802.1X Settings 230
Manage Port Authentication on Individual Ports 232
View the Port Summary. 236
View the Client Summary 237
Set Up Traffic Control 239
Manage MAC Filtering 239
MAC Filter Summary 241
Configure Storm Control Settings 242
Manage Port Security 246
Configure Protected Ports 250
Configure Access Control Lists. 251
Use the ACL Wizard to Create a Simple ACL 251
Configure a Basic MAC ACL 256
Configure MAC ACL Rules 259
Configure MAC Bindings 263
View or Delete MAC ACL Bindings in the MAC Binding Table 265
Configure a Basic or Extended IP ACL. 266
Configure Rules for a Basic IP ACL 269
Configure Rules for an Extended IP ACL 273
Configure IP ACL Interface Bindings 280
View or Delete IP ACL Bindings in the IP ACL Binding Table 282
Configure VLAN ACL Bindings 283

Chapter 6 Monitor the System

Monitor the Switch and the Ports 287
View Switch Statistics 287
View Port Statistics 290
View and Manage Detailed Port Statistics 293
View or Clear EAP and EAPoL Statistics 299
Perform a Cable Test 300
Configure and View Logs 302
Manage the Memory Logs 302
Manage the Flash Log 304
Manage the Server Log 305
View or Clear the Trap Logs and the Counters 308
Configure Port Mirroring 310

Chapter 7 Maintenance

Reboot the Switch 314
Reset the Switch to Its Factory Default Settings 315
Export a File From the Switch 316
Use TFTP to Export a File From the Switch to a TFTP Server 316
Use HTTP to Export a File from the Switch to a Computer 318
Download a File to the Switch or Update the Firmware 319
Use TFTP to Download a File to the Switch or Update the Software Image 319
Use HTTP to Download a File to the Switch or Update the Software Image 321
Manage Software Images 323
Copy a Software Image 324
Configure Dual Image Settings 324
View the Dual Image Status 326
Perform Diagnostics and Troubleshooting 327
Ping an IPv4 Address 327
Send an IPv4 Traceroute 329
Enable Remote Diagnostics 331

Appendix A Configuration Examples

Virtual Local Area Networks (VLANs) 333
VLAN Configuration Examples 334
Access Control Lists (ACLs) 335
MAC ACL Sample Configuration 335
Standard IP ACL Sample Configuration 336
Differentiated Services (DiffServ) 337
Class 338
DiffServ Traffic Classes 339
Creating Policies 339
DiffServ Example Configuration 340
802.1X Access Control 341

802.1X Example Configuration 343
Multiple Spanning Tree Protocol 344
MSTP Example Configuration 346

Appendix B Specifications and Default Settings

Switch Default Settings 349
General Feature Default Settings 350
System Setup and Maintenance Settings 356
Port Characteristics 356
Traffic Control Settings 357
Quality of Service Settings 357
Security Settings 358
System Management Settings 358
Settings for Other Features 359
Hardware Technical Specifications 359

1

Get Started

This user manual describes how you can configure and operate the NETGEAR S350 Series 8-Port Gigabit Ethernet Smart Switch by using the local browser–based management interface.

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

- **GS308T**. S350 Series 8-Port Gigabit Ethernet Smart Switch
- **GS310TP**. S350 Series 8-Port Gigabit PoE+ Ethernet Smart Switch with 2 SFP Ports

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

The chapter contains the following sections:

- Available Publications
- Switch Management and Discovery Overview
- Options to Change the Default IP Address of the Switch
- Discover or Change the Switch IP Address
- About the User Interfaces
- Access the Local Browser Interface
- Navigation Tabs, Configuration Menus, and Page Menu
- Change the Language of the Local Browser Interface
- Use the Device View of the Local Browser Interface
- Interface Naming Conventions
- Configure Interface Settings
- Context-Sensitive Help and Access to the Support WebSite
- Access the User Guide Online
- Register Your Product

Note: In this manual, the local browser–based management interface is referred to as the local browser interface.

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

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

Available Publications

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

- *Installation Guide*
- *Hardware Installation Guide*

Switch Management and Discovery Overview

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

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

- **NETGEAR Smart Control Center (SCC) program**. The SCC runs on a Windows-based computer. You can download the SCC program from netgear.com/support/download/. For more information about the SCC program see Discover the Switch in a Network With a DHCP Server on page 12 and Discover the Switch in a Network Without a DHCP Server on page 13.
- **NETGEAR Switch Discovery Tool**. If you use a Mac computer, you can use the NETGEAR Switch Discovery Tool to discover the switch in your network and access the local browser interface of the switch. For more information about the Switch Discovery Tool, Use the NETGEAR Switch Discovery Tool to Access the Switch on page 15.

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

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

Options to Change the Default IP Address of the Switch

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

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

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

- **Static assignment through the Smart Control Center**. If you connect the switch to a network that does not include a DHCP server, you can use the Smart Control Center to assign a static IP address, subnet mask, and default gateway. For more information, see Discover the Switch in a Network Without a DHCP Server on page 13.
- **Static assignment by connecting from a local host**. If you do not want to use the Smart Control Center to assign a static address, you can connect to the switch from a computer in the 192.168.0.0/24 network and change the settings by using the local browser interface on the switch. For information about how to set the IP address on the computer so that it is in the same subnet as the default IP address of the switch, see Configure a Static IP Address From a Directly Connected Computer on page 16.

Discover or Change the Switch IP Address

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

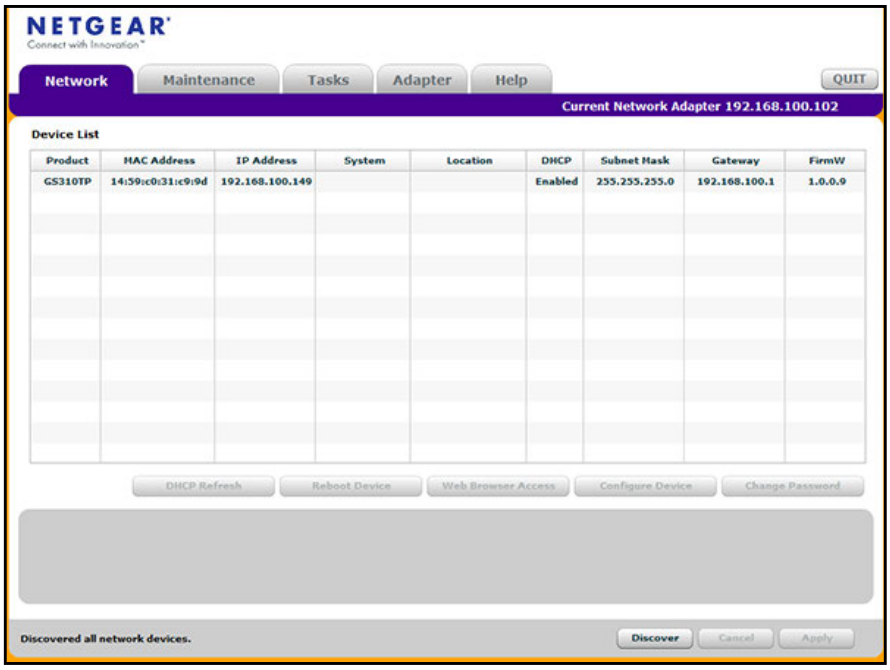
Discover the Switch in a Network With a DHCP Server

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

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

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

1. Connect the switch to a network with a DHCP server.
2. Power on the switch by connecting its power cord.
3. Install the Smart Control Center on your computer.
4. Start the Smart Control Center.
5. Click the **Discover** button for the Smart Control Center to discover all the devices in the subnet.



6. Make a note of the displayed IP address assigned by the DHCP server.

   You can use this IP address later to access the switch directly from a web browser (that is, without using the Smart Control Center).

7. Select your switch by clicking the line that displays the switch.
8. Click the **Web Browser Access** button.

   The Smart Control Center launches a browser that displays the login page of the selected device.

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

Discover the Switch in a Network Without a DHCP Server

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

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

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

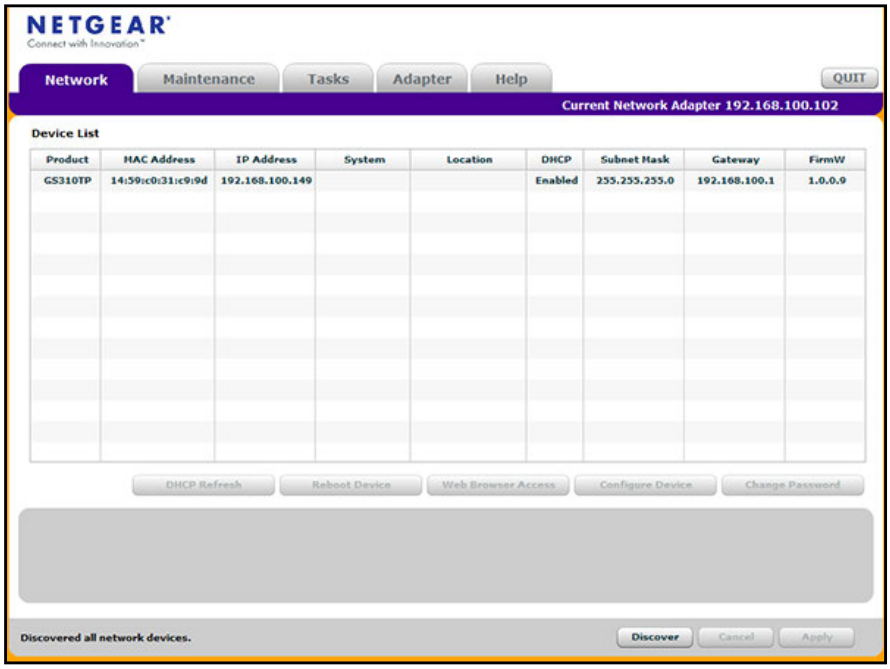
To assign a static IP address:

1. Connect the switch to your existing network.
2. Power on the switch by connecting its power cord.
3. Install the Smart Control Center on your computer.
4. Start the Smart Control Center.
5. Click the **Discover** button for the Smart Control Center to find your switch.

   The utility broadcasts Layer 2 discovery packets within the broadcast domain to discover the switch.
6. Select the switch, and then click the **Configure Device** button.

   The page expands to display additional fields at the bottom.
7. Select the **Disabled** radio button.

   DHCP is disabled.
8. Enter the static switch IP address, gateway IP address, and subnet mask for the switch.



9. Type your password to continue with the configuration change.

   Tip: You must enter the current password each time that you use the Smart Control Center to update the switch settings. The default password is **password**.
10. Click the **Apply** button.

    Your settings are saved.

Use the NETGEAR Switch Discovery Tool to Access the Switch

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

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

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

1. Download the Switch Discovery Tool by visiting netgear.com/support/product/netgear-switch-discovery-tool.aspx.

   Depending on the computer that you are using, download either the Mac version or the version for a 64-bit Windows-based computer.
2. Temporarily disable the firewall, Internet security, antivirus programs, or all of these on the computer that you use to configure the switch.
3. Unzip the Switch Discovery Tool files, double-click the **`.exe`** or **`.dmg`** file (for example, `NETGEAR+Switch+Discovery+Tool+Setup+1.2.101`.exe or `NetgearSDT-V1.2.101.dmg`), and install the program on your computer.

   The installation process places a **NETGEAR Switch Discovery Tool** icon on your desktop.
4. Reenable the security services on your computer.
5. Power on the switch.

   The DHCP server assigns the switch an IP address.
6. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection. The computer and the switch must be on the same Layer 2 network.
7. Open the Switch Discovery Tool.

   To open the program, double-click the **NETGEAR Switch Discovery Too**l icon on your desktop.

   The initial page displays a menu and a button.
8. From the **Choose a connection** menu, select the network connection that allows the Switch Discovery Tool to access the switch.
9. Click the **Start Searching** button.

   The Switch Discovery Tool displays a list of Smart Managed Plus Switches that it discovers on the selected network.

   For each switch, the tool displays the IP address.

10. To access the local browser interface of the switch, click the **ADMIN PAGE** button.

    The login page of the local browser interface opens.

11. Enter the switch password.

    The default password is **password**. The password is case-sensitive.

    The Switch Information page displays.

Configure a Static IP Address From a Directly Connected Computer

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

To configure a static IP address on the switch:

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

   If the DHCP client of the switch is enabled and you remove the switch from the network with the DHCP server, the IP address reverts to the default IP address of 192.168.0.239 with a subnet of 255.255.255.0.

   Note: If you already disabled the DHCP client and assigned a static IP address to the switch, change the IP settings of your computer to be in the same subnet as the static IP address.

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

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

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

2. Connect your computer to the switch using an Ethernet cable.
3. Power on the switch by connecting its power cord.
4. Launch a web browser.
5. In the address field of your web browser, enter the IP address of the switch.

If you did not disable the DHCP client and assigned a static IP address to the switch, enter **192.168.0.239**.

The login window opens.

6. If the browser does not display the login window, do the following:
   - Your browser might display a security message and might not let you proceed. Consider the following examples:
     - **Google Chrome**. If Google Chrome displays a *Your connection is not private* message, click the **ADVANCED** link. Then, click the **Proceed to x.x.x.x (unsafe)** link, in which **x.x.x.x** represents the IP address of the switch.
     - **Mozilla Firefox**. If Mozilla Firefox displays a *Your connection is not secure* message, click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that opens, click the **Confirm Security Exception** button.
     - **Microsoft Internet Explorer**. If Microsoft Internet Explorer displays a *There is a problem with this website's security certificate* message, click the **Continue to this website (not recommended)** link.
     - **Apple Safari**. If Apple Safari displays a *This connection is not private message*, click the **Show Details** button. Then, click the **visit this website** link. If a warning pop-up window opens, click the **Visit Website** button. If another pop-up window opens to let you confirm changes to your certificate trust settings, enter your Mac password and click the **Update Setting** button.
   - Make sure that the switch is receiving power and that its Power LED is lit.
   - Close and reopen the browser.
7. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
8. **Select System > Management > IP Configuration**.

   The IP Configuration page displays.
9. Select the **Static IP Address** radio button.
10. Configure the IP address, subnet mask, and default gateway to be assigned to the switch.
11. Click the **Apply** button.

    Your settings are saved.

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

About the User Interfaces

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

- Local browser interface (which used to be referred to as the web interface)
- Simple Network Management Protocol (SNMP)

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

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

Software Requirements to Use the Local Browser Interface

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

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

Supported Web Browsers

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

- Microsoft Internet Explorer (IE) version 11
- Microsoft Edge
- Mozilla Firefox version 50
- Chrome version 51
- Safari on Windows OS versions 5.1
- Safari on MAC OS X version 10.1

Access the Local Browser Interface

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

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

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

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

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

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

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

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

   The login window opens.
4. If the browser does not display the login window, do the following:
   - If your browser displays a security warning, dismiss the warning by doing one of the following
     - **Google Chrome**. Click the **ADVANCED** link. Then, click the **Proceed to x.x.x.x (unsafe)** link, in which x.x.x.x represents the domain name or IP address of the device.
     - **Apple Safari**. Click the **Show Details** button. Then, click the **visit this website** link. If a warning pop-up window displays, click the **Visit Website** button. If another pop-up window displays to let you confirm changes to your certificate trust settings, enter your Mac user name and password and click the **Update Setting** button.
     - **Mozilla Firefox**. Click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that displays, click the **Confirm Security Exception** button.
     - **Microsoft Edge**: Select **Details > Go on to the webpage**.
     - **Microsoft Internet Explorer**. Click the **Continue to this website (not recommended)** link.
   - If you use a wired Ethernet connection, make sure that the computer is connected to the same network that the switch is attached to or directly to one of the LAN Ethernet ports of the switch.
   - If you use a mobile device, make sure that mobile device is connected to an access point that is attached to the same network that the switch is connected to or that the access point is directly attached to one of the LAN Ethernet ports of the switch.

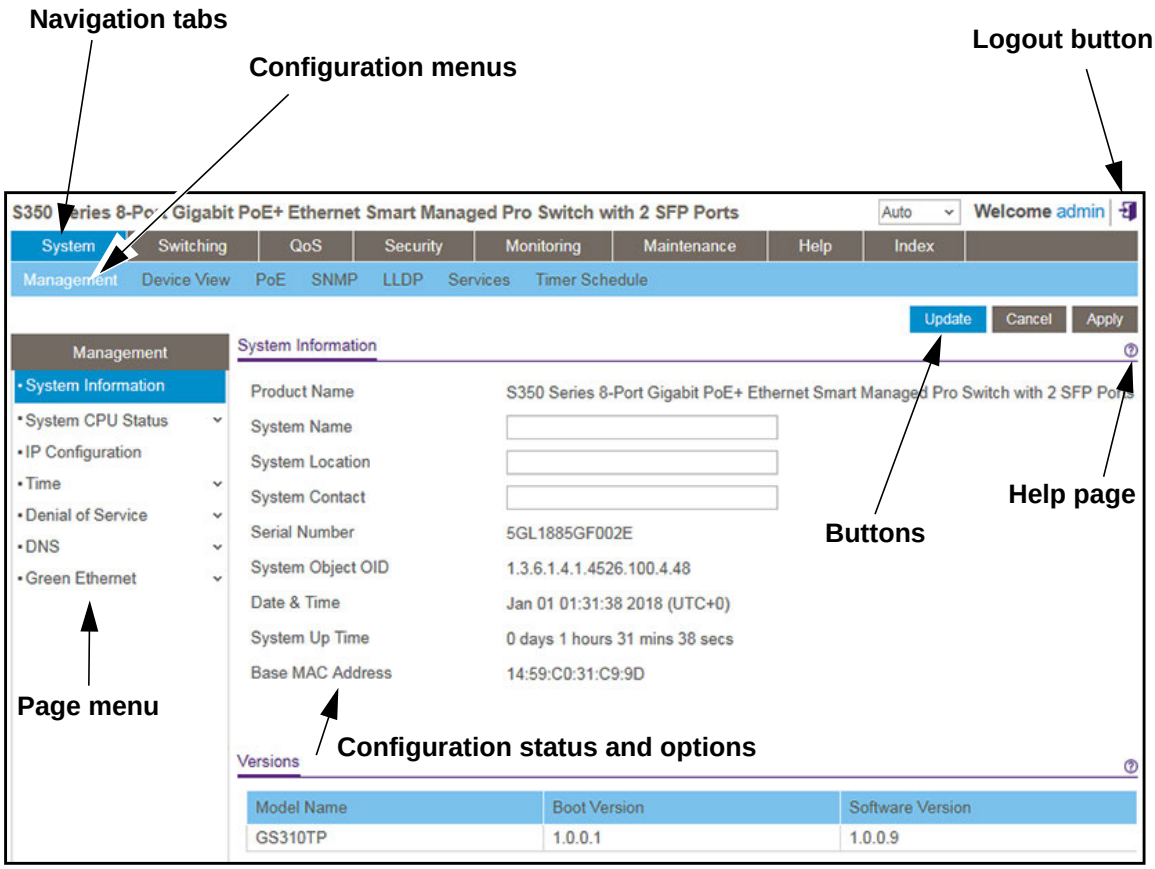
- Make sure that the switch is receiving power and that its Power LED is lit.
- Close and reopen the browser.

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

   The default password is **password**.

   The System Information page displays.

   The following figure shows the layout of the local browser interface.

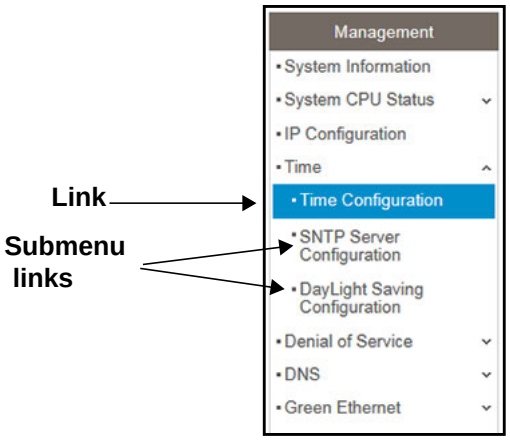


Navigation Tabs, Configuration Menus, and Page Menu

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

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

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



Configuration and Status Options

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

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

Buttons in the Local Browser Interface

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

Table 1. Command buttons in the local browser interface

Button	Function
Add	Clicking the **Add** button adds the new item configured in the heading row of a table.
Apply	Clicking the **Apply** button to save your settings. 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	
\	<
/	>
*	|
?	

Change the Language of the Local Browser Interface

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

To change the language of the local browser interface:

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

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

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

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. At the top of the page, to the left of *Welcome*, select a language from the language menu.

   A confirmation pop-up window opens.
6. Click the **OK** button to confirm.

   The switch restarts and you must log in again.

   The language of the local browser interface is now set to the language that you selected.

Use the Device View of the Local Browser Interface

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

To use Device View:

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

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

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

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

   The login window opens.

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

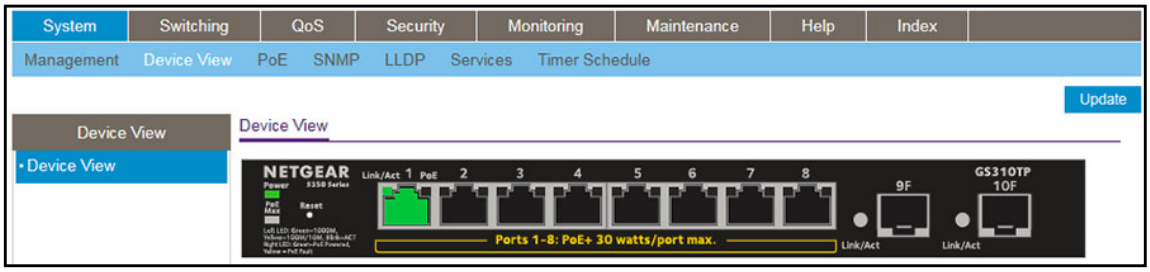
   The default password is **password**.

   The System Information page displays.

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

   The Device View page displays.

   The following figure shows the Device View page for model GS310TP.



   For model GS308T, depending upon the link status of the port, the left port LED and port color in the Device View are either green, yellow, or black:

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

   Model GS308T provides a left port LED but no right port LED.

For model GS310TP, depending on the PoE status of the port, the right port LED and port color in the Device View are either green, yellow, or black:

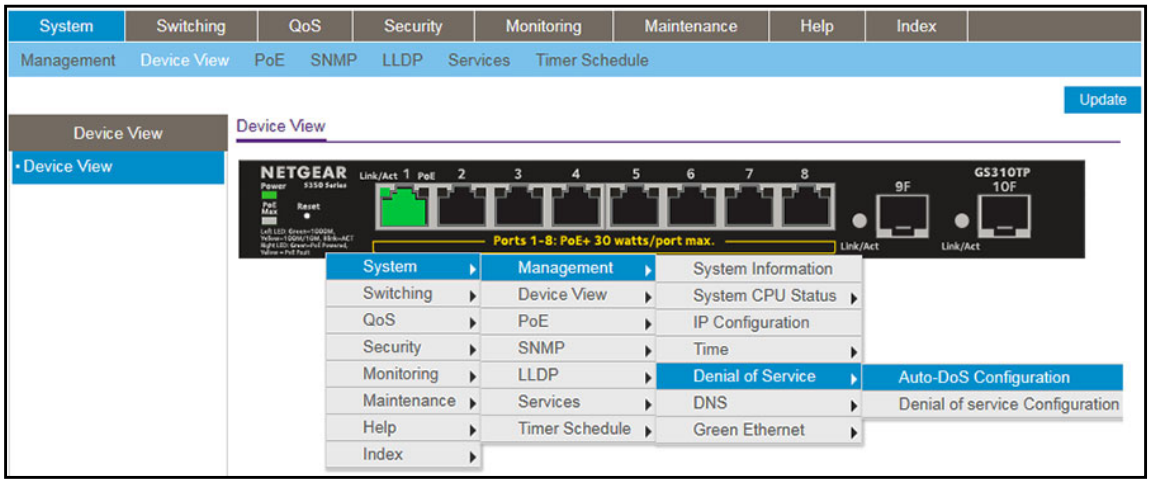
- **Green**. The port is delivering PoE power.
- **Yellow**. A PoE fault occurred.
- **Black**. The port is not delivering PoE power.

6. Click a port to open a menu that displays statistics and configuration options.

   You can select a menu option to access the page that contains the configuration or monitoring options.

   If you right-click the graphic, but do not right-click a specific port, the main menu displays. This menu contains the same options as the navigation tabs at the top of the page.

   The following figure shows the details on the Device View page for model GS310TP.



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

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

Power LED in the Device View

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

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

PoE Max LED in the Device View (Model GS310TP)

The PoE Max LED indicates the following status:

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

Interface Naming Conventions

The switch supports physical and logical interfaces. Interfaces are identified by their type and the interface number. The physical ports are Gigabit interfaces and are numbered on the front panel. You configure the logical interfaces by using the software.

The following table describes the naming convention for all interfaces available on the switch.

Table 3. Naming conventions for interfaces

Interface	Description	Example
Physical	The physical ports are 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. The 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 Access the Local Browser Interface on page 18.

To configure a single port by using the Go To Interface field:

1. Ensure that the page is displaying all ports, and not only the LAGs.
2. In the **Go To Interface** field, type the port number.

   For example, type **g4**.

   For more information, see Interface Naming Conventions on page 25.
3. Click the **Go** button.

   The check box associated with the interface is selected, the row for the selected interface is highlighted, and the interface number displays in the heading row.
4. Configure the desired settings.
5. Click the **Apply** button.

   Your settings are saved.

To configure a single LAG by using the Go To Interface field:

1. Click the **LAG** link or the **All** link to display the LAGs.
2. In the **Go To Interface** field, type the LAG number, for example l3.

   For information, see Interface Naming Conventions on page 25.
3. Click the **Go** button.

   The check box associated with the interface is selected, the row for the selected interface is highlighted, and the interface number appears in the heading row.
4. Configure the desired settings.
5. Click the **Apply** button.

   Your settings are saved.

To configure a single port:

1. Ensure that the page is displaying all ports, and not only the LAGs.
2. Select the check box next to the port number.

   The row for the selected interface is highlighted, and the interface number appears in the heading row.
3. Configure the desired settings.
4. Click the **Apply** button.

   Your settings are saved.

To configure a single LAG:

1. Click the **LAG** link or the **All** link to display the LAGs.
2. Select the check box next to the LAG number.

   The row for the selected interface is highlighted, and the interface number appears in the heading row.
3. Configure the desired settings.
4. Click the **Apply** button.

   Your settings are saved.

To configure multiple ports:

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

   The row for each selected interface is highlighted.
3. Configure the desired settings.
4. Click the **Apply** button.

   Your settings are saved.

To configure multiple LAGs:

1. Click the **LAG** link or the **All** link to display the LAGs.
2. Select the check box next to each LAG to configure.

   The check box associated with each interface is selected, and the row for each selected interface is highlighted.
3. Configure the desired settings.
4. Click the **Apply** button.

   Your settings are saved.

To configure all ports:

1. Ensure that the page is displaying only ports, and not LAGs.
2. Select the check box in the heading row.

   The check boxes for all ports are selected and the rows for all ports are highlighted.
3. Configure the desired settings.
4. Click the **Apply** button.

   Your settings are saved.

To configure all LAGs:

1. Click the **LAG** link to display only the LAG interfaces.
2. Select the check box in the heading row.

   The check box associated with every LAG is selected, and the rows for all LAGs are highlighted.
3. Configure the desired settings.
4. Click the **Apply** button.

   Your settings are saved.

To configure multiple ports and LAGs:

1. Click the **All** link to display all ports and LAGs.
2. Select the check box associated with each port and LAG to configure.

   The rows for the selected ports and LAGs are highlighted.
3. Configure the desired settings.
4. Click the **Apply** button.

   Your settings are saved.

To configure all ports and LAGs:

1. Click the **All** link to display all ports and LAGs.
2. Select the check box in the heading row.

   The check box associated with every port and LAG is selected, and the rows for all ports and LAGs are highlighted.
3. Configure the desired settings.
4. Click the **Apply** button.

   Your settings are saved.

Context-Sensitive Help and Access to the Support WebSite

When you log in to the switch, every page contains a link to the online help (?) that contains information to assist in configuring and managing the switch. The online help pages are context sensitive. For example, if the IP Addressing page is open, the help topic for that page displays if you click the link to the online help.

From the local browser interface, you can access the NETGEAR support website at netgear.com/support.

To access the support website from the local browser interface:

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

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

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

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Help > Support**.

   The Support page displays.
6. To access the NETGEAR support site for the switch, click the **Apply** button.

Access the User Guide Online

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

To access the user manual online from the local browser interface:

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

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

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

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

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Help > Online Help > User Guide**.

   The User Guide page displays.
6. To access the NETGEAR download center, click the **Apply** button**.**
7. Enter the model number of the switch.
8. Locate the user manual on the product support web page.

Register Your Product

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

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

2

Configure System Information

This chapter contains the following sections:

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

View and Configure the Switch Management Settings

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

- View or Define System Information on page 32
- View the System CPU Status on page 35
- Configure the IP Network and VLAN Settings for the Local Browser Interface on page 37
- Configure the Time Settings on page 39
- Configure Denial of Service Settings on page 53
- Configure DNS Settings on page 56
- Configure Green Ethernet Settings on page 60

View or Define System Information

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

To view or define system information:

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

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

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

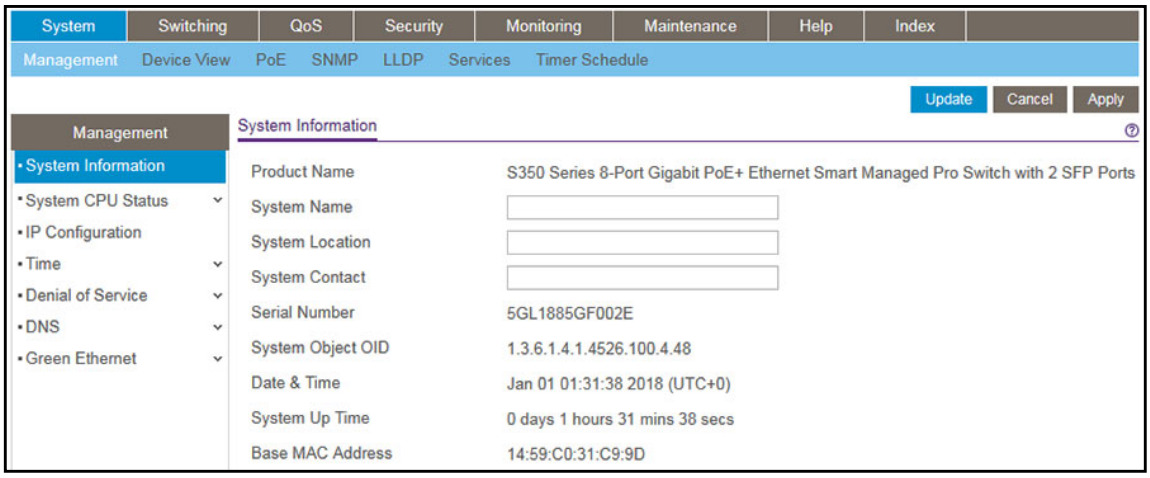
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.



5. Define the following fields:
   - **System Name**. Enter the name to identify this switch. You can use up to 255 alphanumeric characters. The default is blank.
   - **System Location**. Enter the location of this switch. You can use up to 255 alphanumeric characters. The default is blank.
   - **System Contact**. Enter the contact person for this switch. You can use up to 255 alphanumeric characters. The default is blank.
6. Click the **Apply** button.

   Your settings are saved.

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

Table 4. System Information

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.

View the Software Versions

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

To view the software versions:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

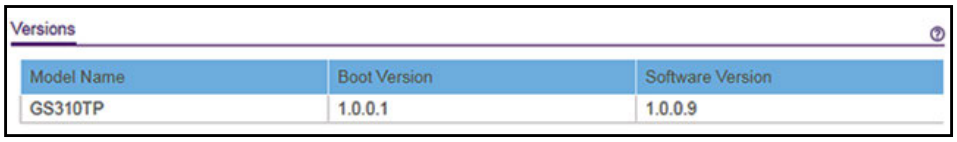
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Scroll down to the Versions section.



6. 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.

Table 5. Versions information

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 software that is running on the switch.

View the System CPU Status

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

To view the system CPU status:

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

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

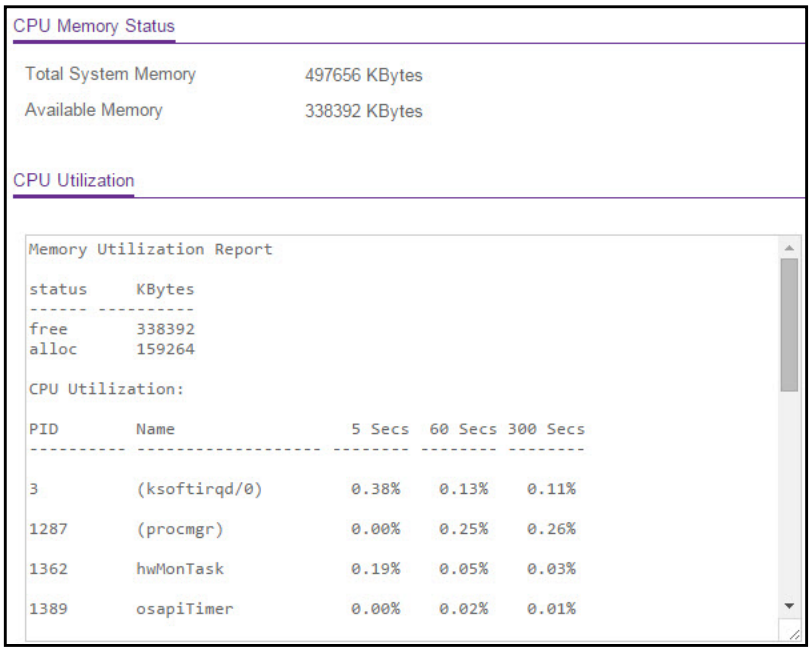
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **System > Management > System CPU Status > System CPU Status**.



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

The following table describes CPU Memory Status information.

Table 6. CPU Memory Status information

Field	Description
Total System Memory	The total memory of the switch in KBytes.
Available Memory	The available memory space for the switch in KBytes.

Configure the CPU Thresholds

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

To configure the CPU thresholds:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **System > Management > System CPU Status > CPU Threshold**.

6. Specify the thresholds:
   - **Rising Threshold**. Notification is generated when the total CPU utilization exceeds this threshold value over the configured time period. The range is 1 to 100.

- **Rising Interval**. This utilization monitoring time period can be configured from 5 to 86400 seconds in multiples of 5 seconds.
- **Falling Threshold**. Notification is triggered when the total CPU utilization falls below this level for a configured period of time.

  The falling utilization threshold must be equal to or less than the rising threshold value. The falling utilization threshold notification is sent only if a rising threshold notification was sent previously. Configuring the falling utilization threshold and time period is optional. If the Falling CPU utilization settings are not configured, the switch uses the same values as the values that are used for the Rising CPU utilization. The range is 1 to 100.
- **Falling Interval**. The utilization monitoring time period can be configured from 5 seconds to 86400 seconds in multiples of 5 seconds.
- **Free Memory Threshold**. The free memory threshold value for the CPU in KB.

7. Click the **Apply** button.

   Your settings are saved.

Configure the IP Network and VLAN Settings for the Local Browser Interface

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

To configure the IP network and VLAN settings for the local browser interface:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **System > Management > IP Configuration**.

The IP Configuration page displays.

6. Select one of the following radio buttons to specify how the network information for the switch must be configured:
   - **Static IP Address**. Specifies that the IP address, subnet mask, and default gateway must be manually configured. Enter this information in the fields below this radio button.
   - **Dynamic IP Address (BOOTP)**. Specifies that the switch must obtain the IP address through a BootP server.
   - **Dynamic IP Address (DHCP)**. Specifies that the switch must obtain the IP address through a DHCP server.
7. If you select the **Static IP Address** radio button, configure the following network information:
   - **IP Address**. The IP address of the network interface. The default value is 192.168.0.239. Each part of the IP address must start with a number other than zero. For example, IP addresses 001.100.192.6 and 192.001.10.3 are not valid.
   - **Subnet Mask**. The IP subnet mask for the interface. The default value is 255.255.255.0.
   - **Default Gateway**. The default gateway for the IP interface. The default value is 192.168.0.254.
8. 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 111.

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.

   Your settings are saved.

Configure the Time Settings

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

Configure the Time Setting Manually

You can view and adjust date and time settings.

To manually configure the time setting:

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

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

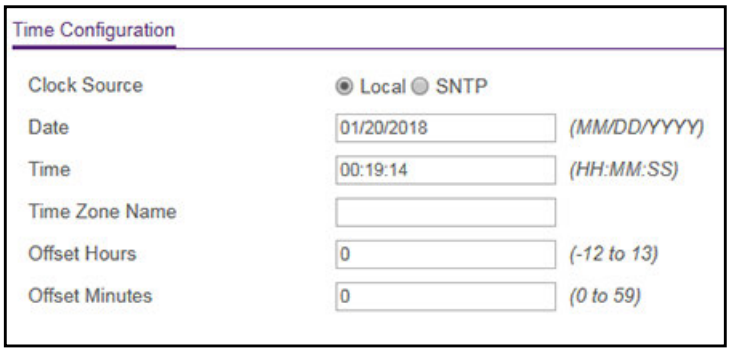
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

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



6. Select the Clock Source **Local** radio button.

7. In the **Date** field, specify the current date by entering the month, day, and year (MM/DD/YYYY).
8. In the **Time** field, specify the current time by entering in hours, minutes, and seconds (HH:MM:SS).

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

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

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

   Note: When 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.

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

    For more information see the description for Time Zone Name in Step 9. The allowed range is –12 to 13. The default value is 0.

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

    For more information see the description for Time Zone Name in Step 9. The allowed range is 0 to 59. The default value is 0.

12. Click the **Apply** button.

    Your settings are saved.

Configure the Time Settings With SNTP and Configure the Global SNTP Settings

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

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

The login window opens.

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

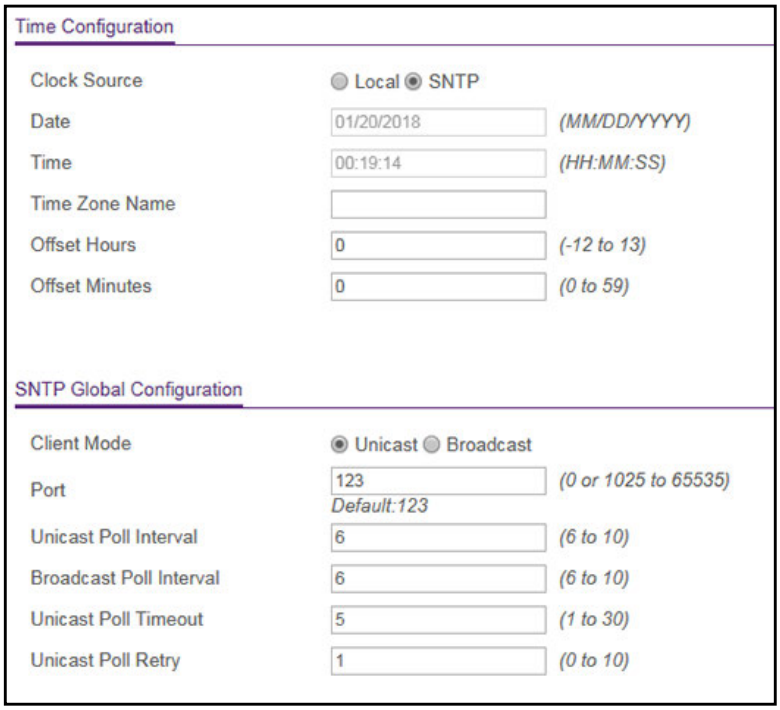
   The default password is **password**.

   The System Information page displays.

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

   The Time Configuration page displays.

6. Select the Clock Source **SNTP** radio button.



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

   - An SNTP server is configured.
   - The switch can contact the SNTP server.

7. Next to Client Mode, select the mode of operation of the SNTP client:
   - **Unicast**. SNTP operates in a point-to-point 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 value is Unicast.

8. If the SNTP client mode is **Unicast**, use the SNTP Server Configuration page to 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 44.

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

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

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

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

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

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

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

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

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

14. In the Time Configuration section (above the SNTP Global Configuration section), configure the following settings:

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

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

       Note: When 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.

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

       For more information see the description for Time Zone Name in Step a. The allowed range is –12 to 13. The default value is 0.

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

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

15. Click the **Apply** button.

    Your settings are saved.

View the SNTP Global Status

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

To view the SNTP global status:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

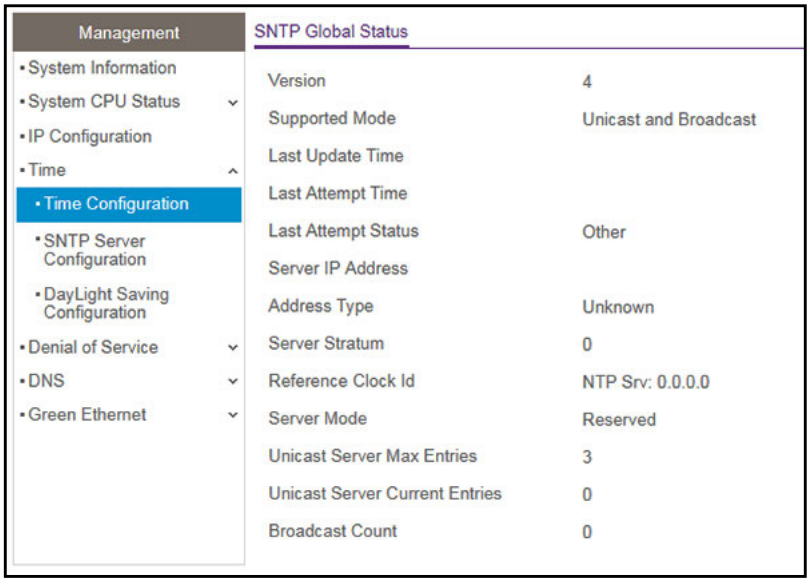
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **System > Management > Time > Time Configuration**.
6. Make sure that the Clock Source **SNTP** radio button is selected.

   The SNTP Global Status section displays below the SNTP Global Configuration section.



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

The following table displays the nonconfigurable SNTP Global Status information.

Table 7. 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.
Last Attempt Status	The status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message was received from a server, a status of **Other** is displayed. These values are appropriate for all operational modes. • **Other**. The status of the last request is unknown. • **Success**. The SNTP operation was successful and the system time was updated. • **Request Timed Out**. After an SNTP request was sent to an SNTP server, the response timer expired before a response from the server was received. • **Bad Date Encoded**. The time provided by the SNTP server is not valid. • **Version Not Supported**. The SNTP version supported by the server is not compatible with the version supported by the client. • **Server Unsynchronized**. The SNTP server is not synchronized with its peers. This is indicated by the leap indicator field in the SNTP message.
Server 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 Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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. From the **Server Type** menu, select the type of SNTP address to enter in the address field.

   The address can be either an IP address (IPv4) or a host name (DNS).

7. In the **Address** field, specify the IP address or the host name of the SNTP server.

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

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

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

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

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

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

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

11. Click the **Add** button.

    The SNTP server entry is added.

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

    You can configure up to three SNTP servers.

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

Table 8. 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: • **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 Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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.

   Your settings are saved.

Remove an SNTP Server

To remove an SNTP server:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The SNTP Server Configuration page displays.

6. Select the check box next to the configured server to remove.
7. Click the **Delete** button.

   The entry is removed, and the device is updated.

Configure Daylight Saving Time Settings

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

To configure the daylight saving time settings:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

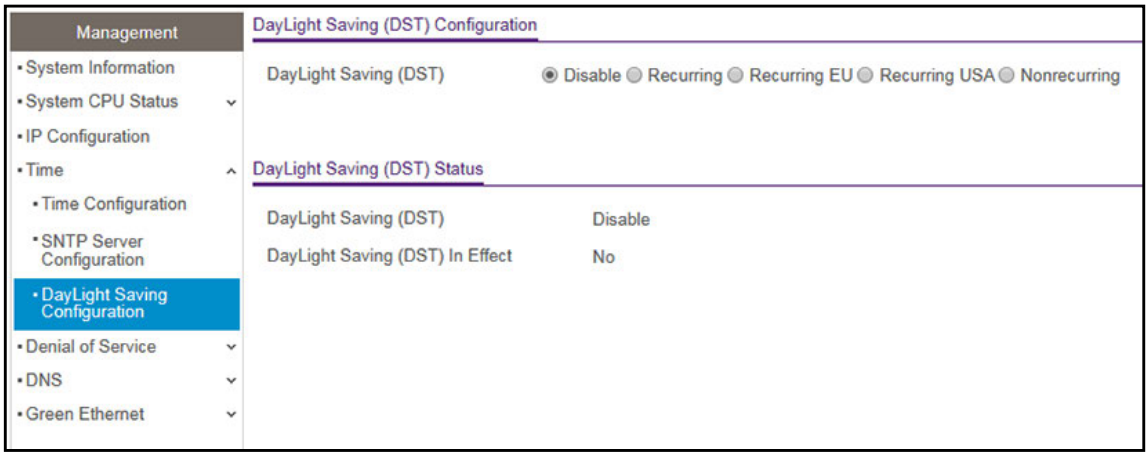
   The login window opens.

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

Table 9. 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. • **Week**. Configure the start week in the month. • **Day**. Configure the start day in the week. • **Month**. Configure the start month. • **Hours**. Configure the start hour. • **Minutes**. Configure the start minutes.
Ends At	These fields are used to configure the end values of date and time. • **Week**. Configure the end week in the month. • **Day**. Configure the end day in the week. • **Month**. Configure the end month. • **Hours**. Configure the end hour. • **Minutes**. Configure the end minutes.
Offset	Configure recurring offset in minutes. The range is from 1 to 1440 minutes.
Zone	Configure the time zone.

   - If you select the DayLight Saving (DST) **Non Recurring** radio button, the fields in the following table are visible and you must configure them.

Table 10. Daylight saving setting is Non Recurring

Field	Description
Begins At	These fields are used to configure the start values of the date and time. • **Month**. Configure the start month. • **Date**. Configure the start date in the month. • **Year**. Configure the start year. • **Hours**. Configure the start hour. • **Minutes**. Configure the start minutes.
Ends At	These fields are used to configure the end values of date and time. • **Month**. Configure the end month. • **Date**. Configure the end date in the month. • **Year**. Configure the end year. • **Hours**. Configure the end hour. • **Minutes**. Configure the end minutes.

Table 10. 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 range is from 1 to 1440 minutes.
Zone	Specify the acronym associated with the time zone when summer time is in effect. This field is not validated against an official list of time zone acronyms.

8. Click the **Apply** button.

   Your settings are saved.

View the DayLight Saving Time Status

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

To view the daylight saving time status:

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

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

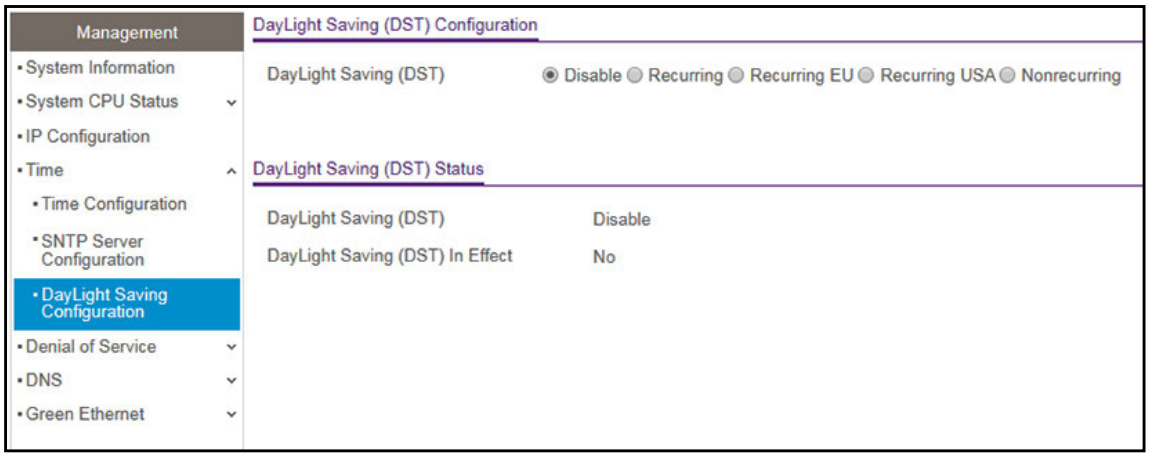
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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. To refresh the page, click the **Update** button.

The following table displays the nonconfigurable daylight saving status information.

Table 11. Daylight Saving (DST) Status information

Field	Description
Daylight Saving (DST)	The Daylight Saving value, which is one of the following: • **Disable** • **Recurring** • **Recurring EU** • **Recurring USA** • **Non Recurring**
Begins At	The start date of daylight saving time. This field is not displayed when daylight saving time is disabled.
Ends At	The end date of daylight saving time. 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	Indicates whether daylight saving time is in effect.

Configure Denial of Service Settings

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

Configure Auto-DoS

You can automatically enable all the DoS features available on the switch, except for the L4 Port attack. For information about the types of DoS attacks the switch can monitor and block, see Configure Denial of Service on page 54.

To enable the Auto-DoS feature:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **System > Management > Denial of Service > Auto-DoS Configuration**.

   The Auto-DoS Configuration page displays.
6. Select the Auto-DoS Mode **Enable** radio button.

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

   Your settings are saved.

Configure Denial of Service

You can select which types of DoS attacks the switch monitors and blocks.

To configure individual DoS settings:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

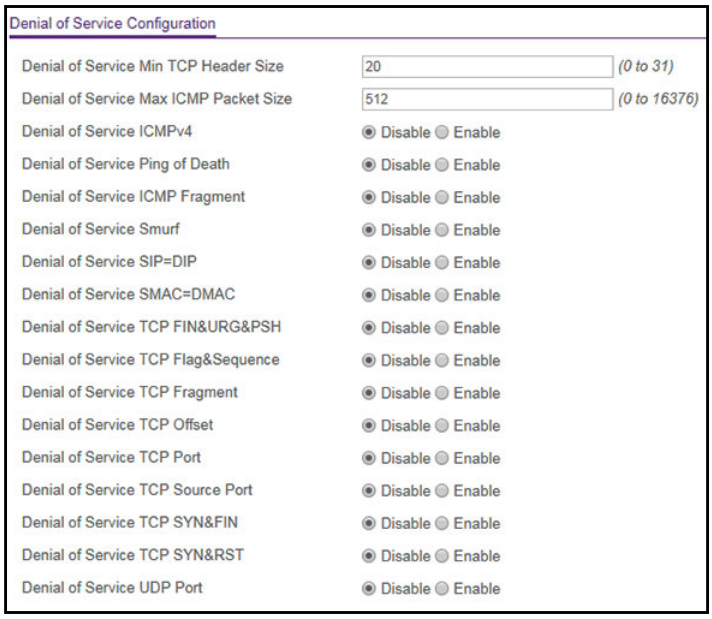
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > Management > Denial of Service > Denial of Service Configuration**.



6. Select the types of DoS attacks for the switch to monitor and block and configure any associated values:
   - **Denial of Service Min TCP Header Size**. Specify the minimum TCP header size allowed. If DoS TCP Fragment is enabled, the switch drops packets with a TCP header smaller than the configured value. The default value is 20.

- **Denial of Service Max ICMPv4 Packet Size**. Specify the maximum ICMPv4 packet size allowed. If ICMPv4 DoS prevention is enabled, the switch drops IPv4 ICMP ping packets with a size greater than the configured value. The default value is 512.
- **Denial of Service 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 Ping of Death**. Enabling Ping of Death DoS prevention causes the switch to drop ICMP ping packet that are larger than 65535 bytes.
- **Denial of Service ICMP Fragment**. Enabling ICMP Fragment DoS prevention causes the switch to drop ICMP fragmented packets.
- **Denial of Service Smurf**. Enabling Smurf DoS prevention causes the switch to drop broadcast ICMP echo request packet.
- **Denial of Service SIP=DIP**. Enabling SIP=DIP DoS prevention causes the switch to drop packets with a source IP address equal to the destination IP address.
- **Denial of Service SMAC=DMAC**. Enabling SMAC=DMAC DoS prevention causes the switch to drop packets with a source MAC address equal to the destination MAC address.
- **Denial of Service TCP FIN&URG&PSH**. Enabling TCP FIN & URG & PSH DoS prevention causes the switch to drop packets with TCP flags FIN, URG, and PSH set and the TCP sequence number equal to 0.
- **Denial of Service TCP Flag&Sequence**. Enabling TCP Flag DoS prevention causes the switch to drop packets with TCP control flags set to 0 and the TCP sequence number set to 0.
- **Denial of Service TCP Fragment**. Enabling TCP Fragment DoS prevention causes the switch to drop packets with a TCP payload for which the IP payload length minus the IP header size is less than the minimum allowed TCP header size.
- **Denial of Service TCP Offset**. Enabling TCP Offset DoS prevention causes the switch to drop packets with a TCP header offset set to 1.
- **Denial of Service TCP Port**. Enabling TCP Port DoS prevention causes the switch to drop packets for which the TCP source port is equal to the TCP destination port.
- **Denial of Service TCP Source Port**. Enabling TCP Source Port DoS prevention causes the switch to drop packets for which the TCP source port number is lower than 1024.
- **Denial of Service TCP SYN&FIN**. Enabling TCP SYN & FIN DoS prevention causes the switch to drop packets with TCP flags SYN and FIN set.
- **Denial of Service TCP SYN&RST**. Enabling TCP SYN & RST DoS prevention causes the switch to drop packets with TCP flags SYN and RST set.
- **Denial of Service UDP Port**. Enabling UDP Port DoS prevention causes the switch to drop packets for which the UDP source port is equal to the UDP destination port.

7. Click the **Apply** button.

   Your settings are saved.

Configure DNS Settings

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

Configure Global DNS Settings and Add a DNS Server

You can configure global DNS settings and DNS server information.

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

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

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

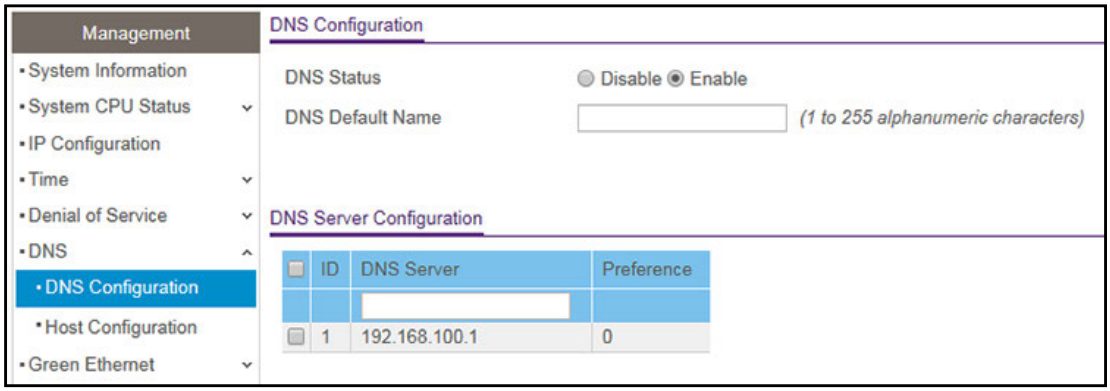
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

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



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

7. In the **DNS Default Name** field, enter the default DNS domain name to include in DNS queries.

   When the system is performing a lookup on an unqualified host name, this field is provides the domain name (for example, if default domain name is netgear.com and the user enters test, then test is changed to test.netgear.com to resolve the name). The name must not be longer than 255 characters.

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

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

10. Click the **Apply** button.

    Your settings are saved.

The following table displays DNS Server Configuration information.

Table 12. 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.

Remove a DNS Server

You can remove a DNS server that you no longer need.

To remove a DNS server:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > Management > DNS > DNS Configuration**.
6. In the DNS Server Configuration table, select the check box for the DNS server.

   Note: If you do not select a DNS server, all the DNS servers are removed after you click the **Delete** button.

7. Click the **Delete** button.

   The DNS server is removed.

Configure and View Host Name-to-IP Address Information

You can manually map host names to IP addresses or view dynamic host mappings.

Add a Static Entry to the Dynamic Host Mapping Table

To add a static entry to the local dynamic host mapping table:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > Management > DNS > Host Configuration**.

   The DNS Host Configuration page displays.

6. In the **Host Name (1 to 255 characters)** field, specify the static host name to add.

   Its length cannot exceed 255 characters and it is a required field.

7. In the **IPv4 Address** field, enter the IP address to associate with the host name.
8. Click the **Add** button.

   Your settings are saved. The entry displays in the Dynamic Host Mapping table.

Remove an Entry From the Dynamic Host Mapping Table

To remove an entry from the Dynamic Host Mapping table:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

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

   The DNS Host Configuration page displays.
6. Select the check box next to the entry to remove.
7. Click the **Delete** button.

   The entry is removed from the Dynamic Host Mapping table.

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

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > Management > DNS > Host Configuration**.

   The DNS Host Configuration page display.

6. Select the check box next to the entry to update.
7. Enter the new information in the appropriate field.
8. Click the **Apply** button.

   Your settings are saved.

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

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

Table 13. 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

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

To configure the Green Ethernet settings:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

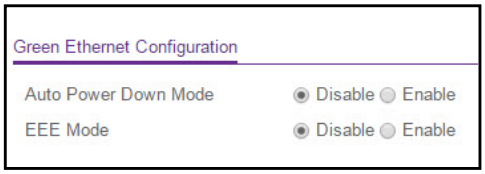
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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



6. Select the Auto Power Down Mode **Disable** or **Enable** radio button.

   By default, this mode is disabled. When a port link is down, the underlying physical layer goes down for a short period and then checks for port link pulses again so that auto-negotiation remains possible. In this way, the switch saves power when no link partner is present for the port.

7. Select the EEE Mode **Disable** or **Enable** radio button.

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

8. Click the **Apply** button.

   Your settings are saved.

Configure Green Ethernet Interface Settings

You can configure Green Ethernet settings for individual interfaces.

To configure the Green Ethernet interface settings:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

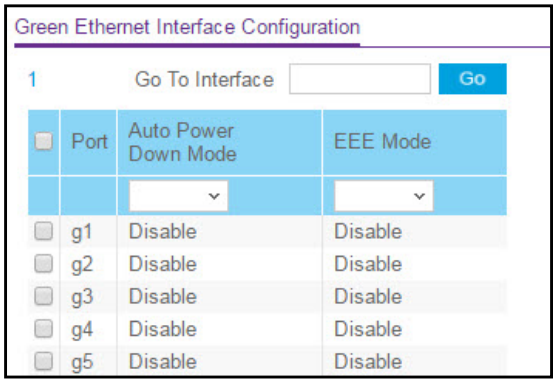
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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



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

7. From the **Auto Power Down Mode** menu, select **Enable** or **Disable**.

   By default, this mode is disabled for the port. When a port link is down, the underlying physical layer goes down for a short period and then checks for port link pulses again so that auto-negotiation remains possible. In this way, the switch saves power when no link partner is present for the port.

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

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

9. Click the **Apply** button.

   Your settings are saved.

Use the Device View

For information about the device view, see Use the Device View of the Local Browser Interface on page 23.

Configure PoE

On model GS310TP, you can configure the global Power over Ethernet (PoE) configuration settings and the PoE settings for each port.

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

Configure the Global PoE Settings

To configure the PoE settings:

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

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

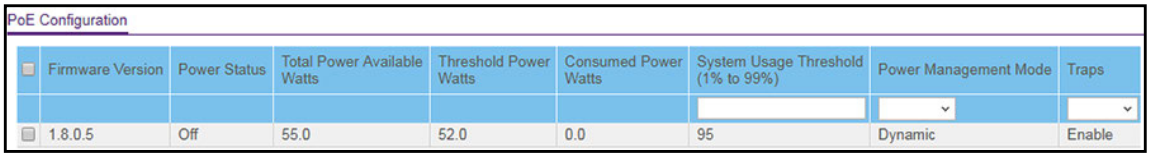
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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**.



The previous figure shows the PoE Configuration page for model GS310TP.

6. In the **System Usage Threshold** field, enter a number from 1 to 99 to set the threshold level at which a trap is sent if the consumed power exceeds the threshold power.
7. From the **Power Management Mode** menu, select the power management algorithm that the switch uses to deliver power to the requesting powered devices (PDs):
   - **Static**. Specifies that the power allocated for each port depends on the type of power threshold configured on the port.
   - **Dynamic**. Specifies that the power consumption on each port is measured and calculated in real time.
8. To active the PoE traps, from the **Traps** menu, select **Enable**.

   Selecting **Disable** deactivates the PoE traps. The default setting is Enabled.
9. Click the **Apply** button.

   Your settings are saved.

The following table describes the nonconfigurable fields on the page.

Table 14. PoE Configuration fields

Field	Description
Firmware Version	The firmware version of the PoE firmware component.
Power Status	The power status.
Total Power Available Watts	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. **Note:** The threshold power value is determined by the value that you enter in the **System Usage Threshold** field.
Consumed Power Watts	The total amount of power in watts that is being delivered to all ports.

Configure the PoE Port Settings

To configure the PoE port settings:

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

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

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

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

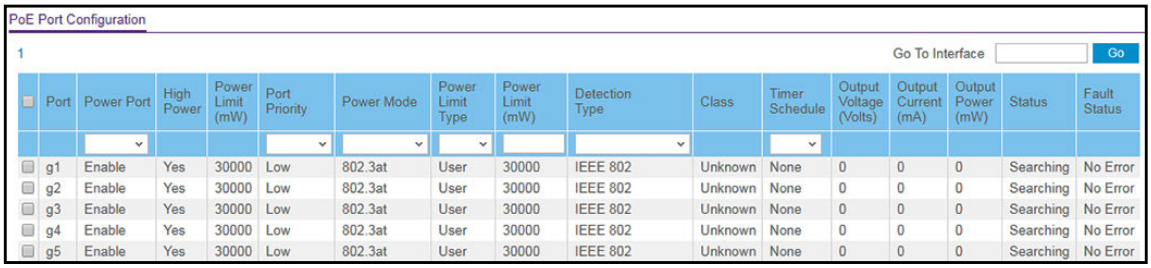
The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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



   The previous figure shows the PoE Port Configuration page for model GS310TP.

6. Select the check boxes for the ports that you want to configure or select the check box in the heading to configure all ports.
7. From the **Port Power** menu, select the PoE mode of the port:
   - **Enable**. The port's capacity to deliver power is enabled. This is the default setting.
   - **Disable**. The port's capacity to deliver power is disabled.
8. From the **Port Priority** menu, select the priority for the port in relation to other ports if the total power that the switch is capable of delivering exceeds the total power budget:
   - **Low**. Low priority. This is the default setting.
   - **Medium**. Medium priority.
   - **High**. High priority.
   - **Critical**. Critical priority.

   The port priority determines which ports can still deliver power after the total power delivered by the switch exceeds the total power budget. (In such a situation, the switch might not be able to deliver power to all connected devices.) If the same priority applies to two ports, the lower-numbered port receives higher priority.
9. From the **Power Mode** menu, select the PoE mode that the port must function in:
   - **802.3af**. The port is powered in and limited to the IEEE 802.3af mode. A PD that requires IEEE 802.3at does not receive power if the port functions in IEEE 802.3af mode.
   - **Legacy**. The port is powered using high-inrush current, which is used by legacy PDs that require more than 15W to power up.
   - **Pre-802.3at**. The port is initially powered in the IEEE 802.3af mode and, before 75 msec pass, is switched to the high power IEEE 802.3at mode. Select this mode if

the PD does not perform Layer 2 classification or if the switch performs 2-event Layer 1 classification.

- **802.3at**. The port is powered in the IEEE 802.3at mode and is backward compatible with IEEE 802.3af. The 802.3at mode is the default mode. In this mode, if the switch detects that the attached PD requests more power than IEEE 802.3af but is not an IEEE 802.3at Class 4 device, the PD does not receive power from the switch.

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

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

11. In the **Power Limit (mW)** field, enter the maximum power (in mW) that the port can deliver.

    The range is 3,000–30,000 mW. The default is 30,000 mW.

12. From the **Detection Type** menu, select how the port detects the attached PD:
    - **IEEE 802**. The port performs a 4-point resistive detection. This is the default setting.
    - **4pt802.3af+legacy**. The port performs a 4-point resistive detection, and if required, continues with legacy detection.
    - **Legacy.** The port performs legacy detection.
13. From the **Timer Schedule** menu, select a timer schedule or select **None**, which is the default selection.

    For information about setting up and configuring PoE timer schedules, see Set Up PoE Timer Schedules on page 94.

14. Click the **Apply** button.

    Your settings are saved.

The following table describes the nonconfigurable fields on the page.

Table 15. PoE Port Configuration

Field	Description
High Power	All ports supports high power mode.
Power Limit (mW)	The maximum power in milliwatts that can be provided by the port.

Table 15. PoE Port Configuration (continued)

Field	Description
Class	The class defines the range of power that a powered device (PD) is drawing from the switch. The class definitions are as follows: • **0**: 0.44–16.2W • **1**: 0.44–4.2W • **2**: 0.44–7.4W • **3**: 0.44–16.2W • **4**: 0.44–31.6W • **Unknown**. The class cannot be detected, or no PD is attached to the port.
Output Voltage (Volts)	The voltage that is delivered to the PD in volts.
Output Current (mA)	The current that is delivered to the PD in mA.
Output Power (mW)	The power that is delivered to the PD in milliwatts.
Status	The operational status of the port: • **Disabled**. No power is delivered. • **Delivering Power**. Power is being drawn by the PD. • **Requesting Power**. The port is requesting power. • **Fault**. A problem occurred with the power. • **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: • **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. • **Startup Failure**. The PD that is connected to the port failed to start up. In this condition, the port does not provide power. • **Over Voltage**. The port was denied power because of a over-voltage lockout. • **Under Voltage**. The port was denied power because of an under-voltage lockout. • **Thermal Shutdown**. The port detected a thermal temperature fault, preventing the port from providing power.

Configure SNMP

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

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

Configure the SNMPv1/v2 Community

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

Add an SNMP Community:

To add an SNMP community:

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

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

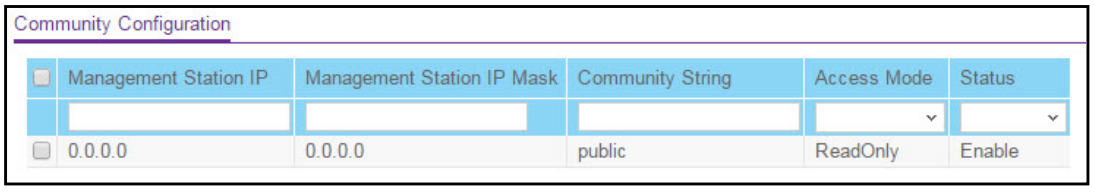
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **System > SNMP > SNMP V1/V2 > Community Configuration**.



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

   Together, the management station IP address and the management station IP mask denote a range of IP addresses from which SNMP clients can use that community to access this device. If either the management station IP address or management station IP mask value is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's address is ANDed with the mask, as is the management station IP address. If the values are equal, access is allowed.

   For example, if the management station IP address and management station IP mask settings are 192.168.1.0/255.255.255.0, any client with an IP address in the range from 192.168.1.0 to 192.168.1.255 (inclusive) is allowed access. To allow access from only one station, use a management station IP mask value of 255.255.255.255, and use that computer's IP address as the client address.
8. In the **Community String** field, specify a community name.
9. From the **Access Mode** menu, select the access level for this community, which is either **Read/Write** or **Read Only**.
10. From the **Status** menu, select to enable or disable the community.

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

    The selected community is added.

Modify an Existing SNMP Community

To modify an existing SNMP community:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

The System Information page displays.

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

   The Community Configuration page displays.

6. Select the check box next to the community.
7. Update the desired fields.
8. Click the **Apply** button.

   Your settings are saved.

Delete an SNMP Community

To delete an SNMP community:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The Community Configuration page displays.

6. Select the check box next to the community to remove.
7. Click the **Delete** button.

   The community is removed.

Configure SNMPv1/v2 Trap Settings

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

Add an SNMP Trap Receiver

To add an SNMP trap receiver:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > SNMP > SNMP V1/V2 > Trap Configuration**.

   The Trap Configuration page displays.

6. In the **Recipients IP** field, enter the IPv4 address at which the SNMP traps from the switch must be received.
7. From the **Version** menu, select the trap version to be used by the SNMP trap receiver.
   - **SNMPv1**. The switch uses SNMPv1 to send traps to the receiver. The default setting is SNMPv1.
   - **SNMPv2**. The switch uses SNMPv2 to send traps to the receiver.
8. In the **Community String** field, specify the name of the SNMP community that includes the SNMP management host and the SNMP agent on the device.

   This name can be up to 16 characters and is case-sensitive.

9. From the **Status** menu, select **Enable** to send traps to the receiver or select **Disable** to prevent the switch from sending traps to the receiver.
10. Click the **Add** button.

    The receiver configuration is added.

Modify Information About an Existing SNMP Recipient

To modify information about an existing SNMP recipient:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

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

   The Trap Configuration page displays.
6. Select the check box next to the recipient.
7. Change the fields as necessary.
8. Click the **Apply** button.

   Your settings are saved.

Delete an SNMP Recipient

To delete an SNMP trap recipient:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

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

   The Trap Configuration page displays.

6. Select the check box next to the recipient to remove.
7. Click the **Delete** button.

   The trap recipient is removed.

Configure SNMPv1/v2 Trap Flags

You can enable or disable traps that the switch can send to an SNMP manager. When the condition identified by an active trap is encountered by the switch, a trap message is sent to any enabled SNMP trap receivers, and a message is written to the trap log.

To configure the trap flags:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **System > SNMP > SNMP V1/V2 > Trap Flags**.

   The Trap Flags page displays.
6. Enable or disable the following system traps:
   - **Authentication**. When enabled, SNMP traps are sent when events involving authentication occur, such as when a user attempts to access the switch local browser interface and does not provide a valid user name and password. The default is Enable.
   - **Link Up/Down**. When enabled, SNMP traps are sent when the administrative or operational state of a physical or logical link changes. The default is Enable.
   - **Spanning Tree**. When enabled, SNMP traps are sent when various spanning tree events occur. The default is Enable.
7. Click the **Apply** button.

   Your settings are saved.

View the Supported MIBs

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

To view the supported MIBs:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

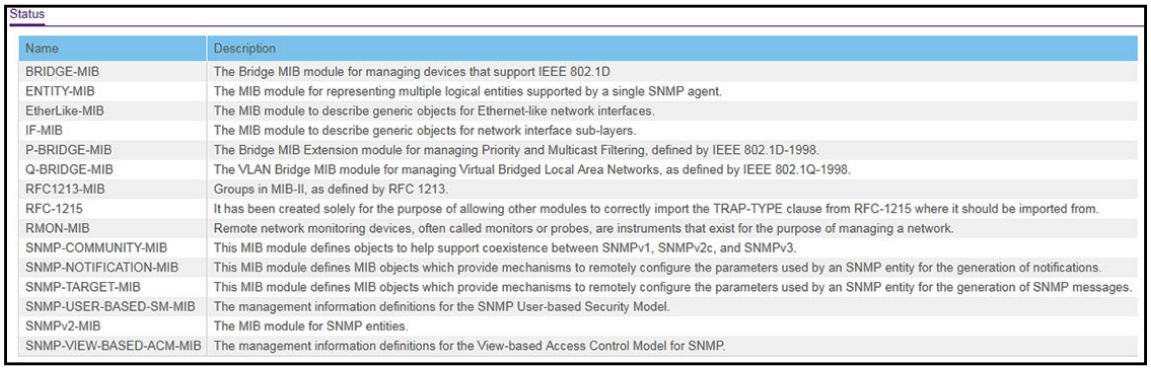
   The login window opens.

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
BRIDGE-MIB	The Bridge MIB module for managing devices that support IEEE 802.1D
ENTITY-MIB	The MIB module for representing multiple logical entities supported by a single SNMP agent.
EtherLike-MIB	The MIB module to describe generic objects for Ethernet-like network interfaces.
IF-MIB	The MIB module to describe generic objects for network interface sub-layers.
P-BRIDGE-MIB	The Bridge MIB Extension module for managing Priority and Multicast Filtering, defined by IEEE 802.1D-1998.
Q-BRIDGE-MIB	The VLAN Bridge MIB module for managing Virtual Bridged Local Area Networks, as defined by IEEE 802.1Q-1998.
RFC1213-MIB	Groups in MIB-II, as defined by RFC 1213.
RFC-1215	It has been created solely for the purpose of allowing other modules to correctly import the TRAP-TYPE clause from RFC-1215 where it should be imported from.
RMON-MIB	Remote network monitoring devices, often called monitors or probes, are instruments that exist for the purpose of managing a network.
SNMP-COMMUNITY-MIB	This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2c, and SNMPv3.
SNMP-NOTIFICATION-MIB	This MIB module defines MIB objects which provide mechanisms to remotely configure the parameters used by an SNMP entity for the generation of notifications.
SNMP-TARGET-MIB	This MIB module defines MIB objects which provide mechanisms to remotely configure the parameters used by an SNMP entity for the generation of SNMP messages.
SNMP-USER-BASED-SM-MIB	The management information definitions for the SNMP User-based Security Model.
SNMPv2-MIB	The MIB module for SNMP entities.
SNMP-VIEW-BASED-ACM-MIB	The management information definitions for the View-based Access Control Model for SNMP.

The following table describes the SNMP Supported MIBs Status fields.

Table 16. 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 Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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 for the Local Browser Interface on page 199.

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

   Your settings are saved.

Configure LLDP

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

The following sections describe how you can configure LLDP:

- Configure LLDP Global Settings on page 76
- Configure LLDP Port Settings on page 78
- View the LLDP-MED Network Policy on page 79
- Configure LLDP-MED Port Settings on page 81
- View the Local Information Advertised Through LLDP on page 82
- View LLDP Neighbors Information on page 84

LLDP is a one-way protocol without any request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function. The transmit and receive functions can be enabled or disabled separately per port. By default, both transmit and receive are disabled on all ports. The application is responsible for starting each transmit and receive state machine appropriately, based on the configured status and operational state of the port.

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

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

Configure LLDP Global Settings

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

To configure global LLDP settings:

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

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

2. Launch a web browser.

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

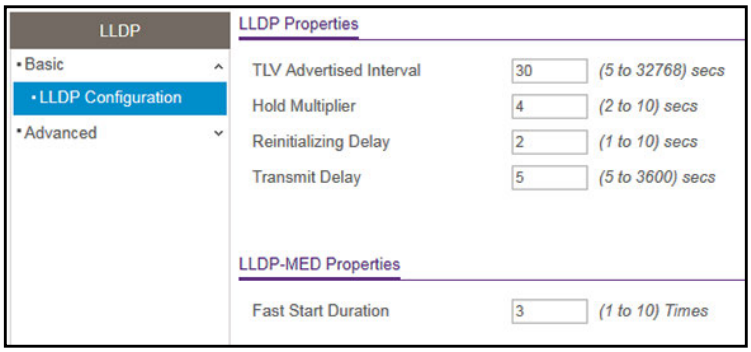
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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



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

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

   This value sets the number of LLDP packets sent when the LLDP-MED fast start mechanism is initialized, which occurs when a new endpoint device links with the LLDP-MED network connectivity device.

8. Click the **Apply** button.

   Your settings are saved.

Configure LLDP Port Settings

You can specify per-interface LLDP settings.

To configure the LLDP interface:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

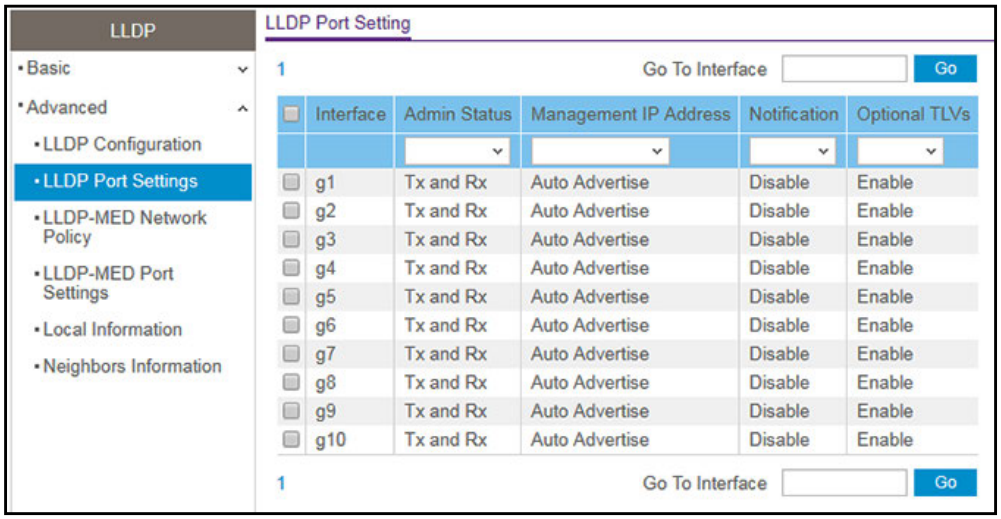
   The login window opens.

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**.



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

7. Use the following menus to configure the LLDP settings for the selected ports:
   - **Admin Status**. Select the status for transmitting and receiving LLDP packets:
     - **Tx Only**. Enable only transmitting LLDP PDUs on the selected ports.
     - **Rx Only**. Enable only receiving LLDP PDUs on the selected ports.
     - **Tx and Rx**. Enable both transmitting and receiving LLDP PDUs on the selected ports.
     - **Disabled**. Do not transmit or receive LLDP PDUs on the selected ports.

     The default is Tx and Rx.
   - **Management IP Address**. Choose whether to advertise the management IP address from the interface. The possible field values are as follows:
     - **Stop Advertise**. Do not advertise the management IP address from the interface.
     - **Auto Advertise**. Advertise the current IP address of the device as the management IP address.

     The default is **Auto Advertise**.
   - **Notification**. When notifications are enabled, LLDP interacts with the trap manager to notify subscribers of remote data change statistics. The default is Disable.
   - **Optional TLVs**. Enable or disable the transmission of optional type-length value (TLV) information from the interface. The default is Enable. The TLV information includes the system name, system description, system capabilities, and port description.

     For information about how to configure the system name, see View and Configure the Switch Management Settings on page 32. For information about how to configure the port description, see Configure the Port Settings and Maximum Frame Size on page 103.
8. Click the **Apply** button.

   Your settings are saved.

View the LLDP-MED Network Policy

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

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

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

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

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

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

The login 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 the LLDP-MED network policy information that displays on the page.

Table 17. LLDP-MED network policy information

Field	Description
Network Policy Number	The policy number.
Application	The media application type associated with the policy, which can be one of the following: • Unknown • Voice • Guest Voice • Guest Voice Signaling • Softphone Voice • Video Conferencing • Streaming Video • Video Signaling A port can receive multiple application types. The application information is displayed only if a network policy TLV was transmitted from the port.
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 Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **System > LLDP > Advanced > LLDP-MED Port Settings**.

   The LLDP-MED Port Settings page displays.
6. From the **Port** menu, select the port to configure.
7. Use the following menus to enable or disable the following LLDP-MED settings for the selected port:
   - **LLDP-MED Status**. The administrative status of LLDP-MED on the interface. When LLDP-MED is enabled, the transmit and receive function of LLDP is effectively enabled on the interface.
   - **Notification**. When Notification is enabled, the port sends a topology change notification if a device is connected or removed.
   - **MED Capabilities**. When MED Capabilities is enabled, the port transmits the capabilities type length values (TLVs) in the LLDP PDU frames.
   - **Network Policy.** When Network Policy is enabled, the port transmits the network policy TLV in LLDP frames.
   - **Extended MDI-PSE**. When Extended MDI-PSE is enabled, the port transmits the extended PSE TLV in LLDP frames.
8. Click the **Apply** button.

   Your settings are saved.

View the Local Information Advertised Through LLDP

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

To view local LLDP information:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

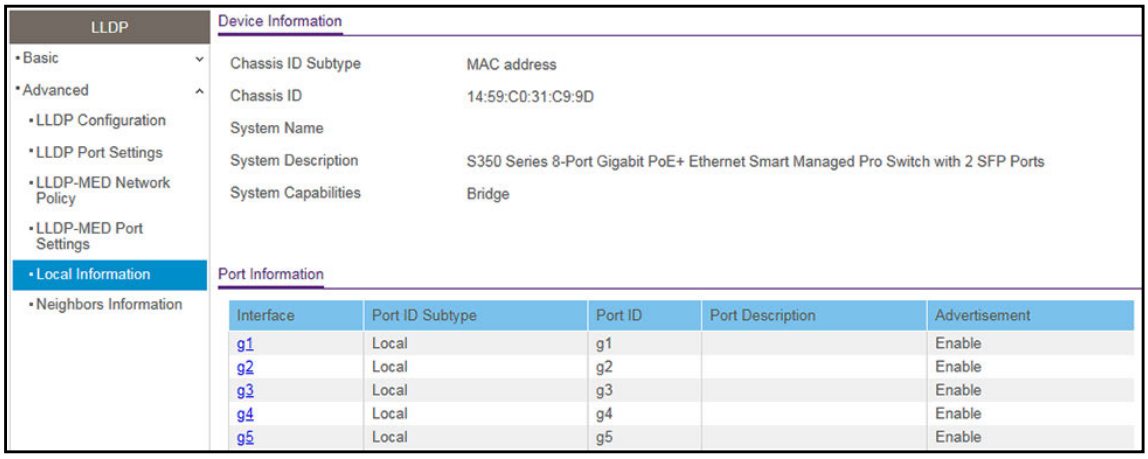
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > LLDP > Advanced > Local Information**.



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

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

Field	Description
Device Information	
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.

Field	Description
System Name	The user-configured system name for the switch.
System Description	The switch description, which includes information about the product model and platform.
System Capabilities	The primary functions that the switch supports.
Port Information	
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 the Port Settings and Maximum Frame Size on page 103.
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 option is True (enabled) or False (disabled).
Auto Negotiation Enabled	The port speed autonegotiation support status. The option is True (enabled) or False (disabled).
Auto Negotiation Advertised Capabilities	The port speed autonegotiation capabilities such as 1000BASE-T half-duplex mode or 100BASE-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.

Field	Description
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.
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 specified interface received from other LLDP-enabled systems.

To view LLDP information received from a neighbor device:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

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

   The Neighbors Information page displays.

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

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.

6. 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 option is True (enabled) or False (disabled).
Auto-Negotiation Enabled	The port speed autonegotiation support status. The option is True (enabled) or False (disabled).
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: • Endpoint Class 1 Indicates a generic endpoint class, offering basic LLDP services. • Endpoint Class 2 Indicates a media endpoint class, offering media streaming capabilities as well as all Class 1 features. • Endpoint Class 3 Indicates a communications device class, offering all Class 1 and Class 2 features plus location, 911, Layer 2 switch support, and device information management capabilities.
PoE Device Type	The port PoE type. For example, Powered.
PoE Power Source	The port's power source.
PoE Power Priority	The port's power priority.
PoE Power Value	The port's power value.
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.

Field	Description
Model Name	The model name advertised by the remote device.
Asset ID	The asset ID advertised by the remote device.
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	The 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.

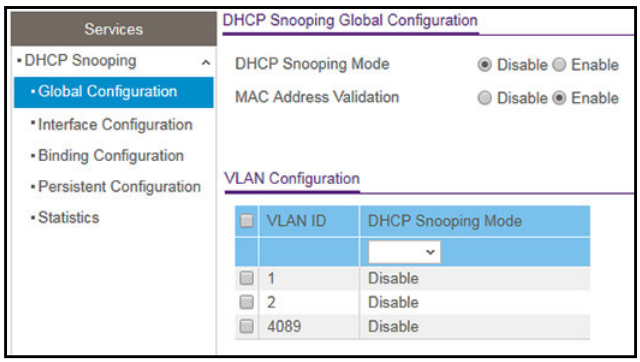
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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**.



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

   The default is Disable.
7. To enable the verification of the sender's MAC address for DHCP snooping, leave the MAC Address Validation **Enable** radio button selected.

   The default is Enable.

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

8. Click the **Apply** button.

   Your settings are saved.

Enable DHCP for All Interfaces in a VLAN

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

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The DHCP Snooping Global Configuration page displays.

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

   Your settings are saved.

Configure DHCP Snooping Interface Settings

You can view and configure each port as a trusted or untrusted port. Any DHCP responses received on a trusted port are forwarded. If a port is configured as untrusted, any DHCP (or BootP) responses received on that port are discarded.

To configure DHCP snooping interface settings:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

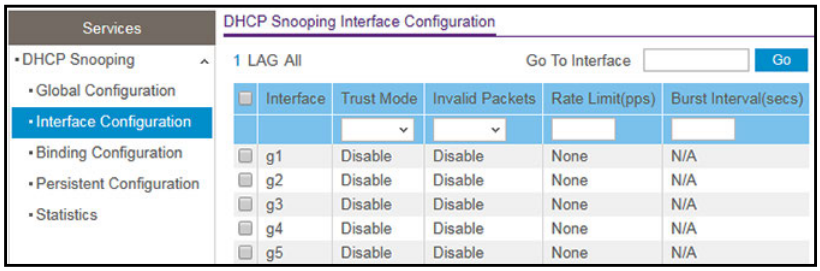
   The login window opens.

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 (DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) are dropped.
     - DHCPRELEASE and DHCPDECLINE messages are dropped if the MAC address is in the snooping database but the binding's interface is other than the interface where the message was received.

  - DHCP packets are dropped when the source MAC address does not match the client hardware address if MAC address validation is globally enabled.
- **Enabled**. The interface is considered to be trusted and forwards DHCP server messages without validation.

8. From the **Invalid Packets** menu, select the packet logging mode.

   When enabled, the DHCP snooping feature generates a log message when an invalid packet is received and dropped by the interface.

9. In the **Rate Limit (pps)** field, specify the rate limit value for DHCP snooping purposes.

   If the incoming rate of DHCP packets per second exceeds the configured burst interval per second, the port shuts down. If the rate limit value is None, he burst interval is also nonapplicable, and rate limiting is disabled.

10. In the **Burst Interval (secs)** field, specify the burst interval value for rate limiting purposes on the interface.

    If the rate limit is N/A, then the burst interval is also nonapplicable, and the field displays N/A.

11. Click the **Apply** button.

    Your settings are saved.

Configure Static DHCP Bindings

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

To 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 Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

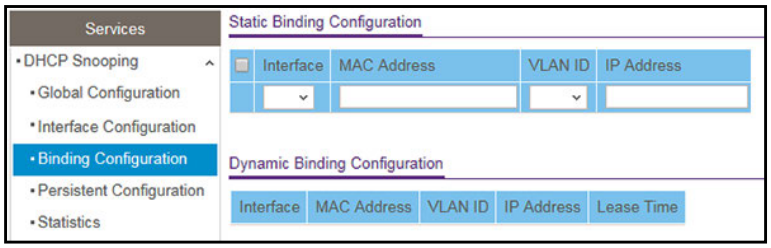
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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



6. From the **Interface** menu, select the interface on which the DHCP client is authorized.
7. In the **MAC Address** field, specify the MAC address for the binding to be added.

   This is the key to the binding database.
8. From the **VLAN ID** menu, select the ID of the VLAN that the client is authorized to use.
9. In the **IP Address** field, specify the IP address of the client.
10. Click the **Add** button.

    The DHCP snooping binding entry is added to the database.

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 18. 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.

Configure DHCP Snooping Persistent Settings

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

To configure DHCP snooping persistent settings:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The Persistent Configuration page displays.

6. Specify where the DHCP snooping bindings database is located.
   - **Local**. The binding table is stored locally on the switch.
   - **Remote**. The binding table is stored on a remote TFTP server.

     If the database is stored on a remote server, specify the following information:

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

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

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

8. Click the **Apply** button.

   Your settings are saved.

View or Clear DHCP Snooping Statistics

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

To view or clear the DHCP snooping statistics:

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

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

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

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

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The DHCP Snooping Statistics page displays.

6. Click the **Clear** button to clear all interfaces statistics.

The following table describes the DHCP snooping statistics.

Table 19. DHCP Snooping Statistics information

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

Set Up PoE Timer Schedules

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

After you create a timer schedule, you can associate it with one or more PoE ports (see Configure the PoE Port Settings on page 64). You can use a separate timer schedule for each PoE port.

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

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

Create a PoE Timer Schedule

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

To create a PoE timer schedule:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **System > Timer Schedule > Basic > Global Configuration**.

   The Timer Schedule Name page displays.
6. In the **Timer Schedule Name** field, specify the name for a timer schedule.
7. Click the **Add** button.

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

Specify the Settings for an Absolute PoE Timer Schedule

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

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

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

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

   The Timer Schedule Configuration page displays.
6. In the Timer Schedule Selection section, make your selections from the following menus:
   a. **Timer Schedule Name**. Select the name of the timer schedule that you want to configure.

      You can select only names of schedules that you created (see Create a PoE Timer Schedule on page 95).

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

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

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

      Selecting an existing entry lets you make changes to that entry.
7. In the Timer Schedule Configuration section, specify the times and dates:
   a. In the **Time Start** field, enter the time of day in the HH:MM format to specify when the timer schedule must start.
   b. In the **Time End** field, enter the time of day in the HH:MM format to specify when the timer schedule must stop.
   c. Next to the **Date Start** field, click the calendar icon and use the menus in the pop-up window to enter the date in the DD-Mon-YYY format to specify when the timer schedule must start.
   d. Next to the **Date End** field, click the calendar icon and use the menus in the pop-up window to enter the date in the DD-Mon-YYY format to specify when the timer schedule must stop.
8. Click the **Add** button.

   The entry for the timer schedule is added.

Specify the Settings for a Recurring PoE Timer Schedule

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

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

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

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The Timer Schedule Configuration page displays.

6. In the Timer Schedule Selection section, make your selections from the following menus:
   a. **Timer Schedule Name**. Select the name of the timer schedule that you want to configure.

      You can select only names of schedules that you created (see Create a PoE Timer Schedule on page 95).

   b. **Timer Schedule Type**. Select **Periodic**.

      The fields in the Timer Schedule Configuration section might adjust to let you configure a timer schedule with a recurrence pattern.

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

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

7. In the Timer Schedule Configuration section, specify the recurrence pattern:
   a. In the **Time Start** field, enter the time of day in the HH:MM format to specify when the timer schedule must start.

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

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

d. Either select the **No End Date** radio button or select the **End Date** radio button, and next to the **End Date** field, click the calendar icon and use the menus in the pop-up window to enter the date in the DD-Mon-YYY format to specify when the timer schedule must stop.

e. From the **Recurrence Pattern** menu, select the pattern:

- **Daily**. The timer schedule works with daily recurrence. The fields adjust.

  Either select the **Every Weekday** radio button to let the schedule operate from Monday through Friday or select the **Every Day(s)** radio button and enter a number from 0 to 255 in the field.

  In the latter case, the schedule is triggered every specified number of days. If the number of days is not specified, or if you enter 0, then the schedule is triggered only once.

- **Weekly**. The timer schedule works with weekly recurrence. The fields adjust.

  In the **Every Week(s)** field, enter a number from 0 to 255 to specify that the schedule must be triggered every specified number of weeks. If the number of weeks is not specified, or if you enter 0, then the schedule is triggered only once.

  Select a single **Week Day** check box, multiple check boxes, or all check boxes to specify the day or days of the week that the schedule must operate.

- **Monthly**. The timer schedule works with monthly recurrence. The fields adjust.

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

  In the **Every Month(s)** field, enter a number from 0 to 99 to specify that the schedule must be triggered every specified number of months. If the number of months is not specified, or if you enter 0, then the schedule is triggered only once.

8. Click the **Add** button.

The entry for the timer schedule is added.

Change the Settings for a Recurring PoE Timer Schedule Entry

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

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

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

   The Timer Schedule Configuration page displays.
6. From the **Timer Schedule Name** menu, select the schedule name.
7. From the **Timer Schedule Type** menu, select the schedule type.
8. From the **Timer Schedule Entry** menu, select the schedule entry.
9. Make the changes to the schedule entry.

   For more information, see Specify the Settings for a Recurring PoE Timer Schedule on page 97.
10. Click the **Apply** button.

    Your settings are saved.

Delete a PoE Timer Schedule Entry

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

To delete a PoE timer schedule entry:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

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

   The Timer Schedule Configuration page displays.
6. From the **Timer Schedule Name** menu, select the schedule name.
7. From the **Timer Schedule Type** menu, select the schedule type.
8. From the **Timer Schedule Entry** menu, select the schedule entry.
9. Click the **Delete** button.

   The entry is deleted.

Delete a PoE Timer Schedule

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

To delete a PoE timer schedule:

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

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

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

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The Timer Schedule Name page displays.

6. Select the check box for the schedule that you want to delete.
7. Click the **Delete** button.

   The schedule is deleted.

3

Configure Switching

This chapter contains the following sections:

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

Configure the Port Settings and Maximum Frame Size

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

To configure the port settings and maximum frame size:

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

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

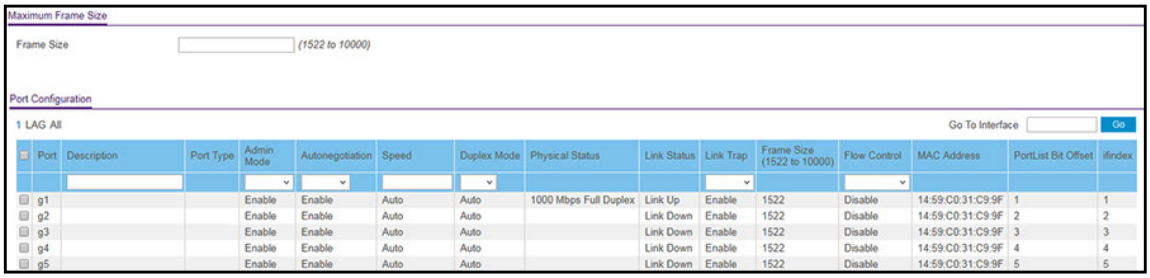
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Ports > Port Configuration**.



6. In the **Frame Size** field, specify the maximum Ethernet frame size that each interface can support.

   The frame size includes the Ethernet header, CRC, and payload. The range is 1522 to 10000. The default maximum frame size is 1522.
7. 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.

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

   The string can be up to 64 characters in length.

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

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

10. From the **Autonegotiation** menu, select **Enable** or **Disable**.

    This selection specifies the autonegotiation mode for the port. The default is Enable.

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

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

    Possible field values are as follows:

    - **Auto**. All supported speeds.
    - **10**. 10 Mbits/second
    - **100**. 100 Mbits/second

    The delimiter characters for setting different speed values are a comma (,), a period (.) and a space ( ). For you to set the autonegotiation speed, the autonegotiation mode must be set to **Enable**. The default is Auto.

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

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

    The options are as follows:

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

    The default is Auto.

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

13. From the **Link Trap** menu, select whether or not to send a trap when the link status changes.

    By default, the switch sends a link trap.

14. From the **Flow Control** menu, select the configuration for IEEE 802.3 flow control.

- **Disable**. If the port buffers become full, the switch does not send pause frames, and data loss could occur. This is the default setting.
- **Symmetric**. If the port buffers become full, the switch sends pause frames to stop traffic.

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

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

15. Click the **Apply** button.

Your settings are saved.

The following table describes the nonconfigurable data that is displayed.

Table 20. Port Configuration information

Field	Description
Port Type	For normal ports this field is blank. Otherwise, the options are as follows: • **Mirrored**. The port is a mirrored port on which all the traffic is copied to the probe port. • **Probe**. Use the 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	The port speed and duplex mode.
Link Status	Indicates whether the link is up or down.
Frame Size (1522 to 10000)	The maximum Ethernet frame size that each interface can support. The frame size depends on your selection from the **Frame Size** menu above the table and applies to each interface.
MAC Address	The physical address of the specified interface.
PortList Bit Offset	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 the 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. By default, the LAG becomes a member of the default management VLAN (that is, VLAN 1).

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

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

Model GS308T and model GS310TP support eight LAGs each.

Configure LAG Settings

You can group one or more full-duplex Ethernet links to be aggregated together to form a link aggregation group, which is also known as a port channel. The switch treats the LAG as if it were a single link.

To configure LAG settings:

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

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

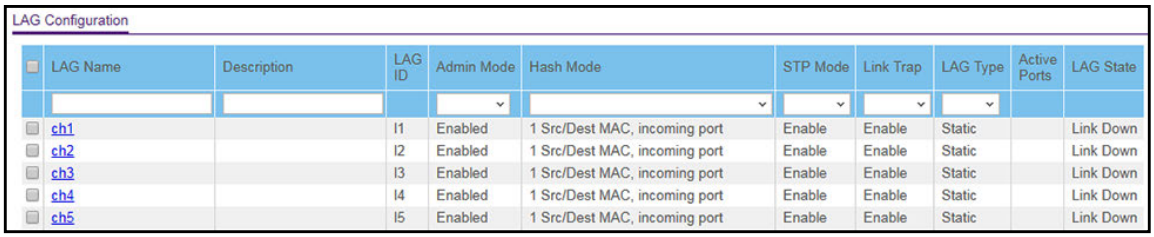
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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**.



6. In the **LAG Name** field, enter a name for the LAG.

   You can enter any string of up to 15 alphanumeric characters.

7. In the **Description** field, enter the description string to be attached to 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 **Hash Mode** menu, select the load-balancing mode for a port channel (LAG):
   - **1 Src/Dest MAC, incoming port**. This mode uses the source MAC address, destination MAC address, and incoming port that are associated with the packet.
   - **2 Src/Dest IP and TCP/UDP Port Fields**. This mode uses the source and destination IP addresses and source and destination TCP or UDP port values that are associated with the packet.

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

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

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

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

12. From the **LAG Type** menu, select **Static** or **LACP**:
    - **Static**. Disables Link Aggregation Control Protocol (LACP) on the selected LAG. The LAG is configured manually. The default is Static.
    - **LACP**. Enables LACP on the selected LAG. The LAG is configured automatically.

13. Click the **Apply** button.

    Your settings are saved.

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

Table 21. 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 Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

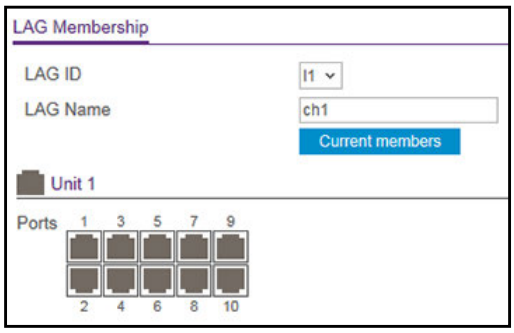
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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



The previous figure shows the LAG Membership page for model GS310TP.

6. From the **LAG ID** menu, select the LAG ID.
7. In the **LAG Name** field, enter the name to be assigned to the LAG.

   You can enter any string of up to 15 alphanumeric characters. You can also use the default name.
8. In the Ports table, click each port that you want to include as a member of the selected LAG.

   A selected port is displayed by a check mark.
9. Click the **Apply** button.

   Your settings are saved.

Set the LACP System Priority

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

To configure LACP:

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

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

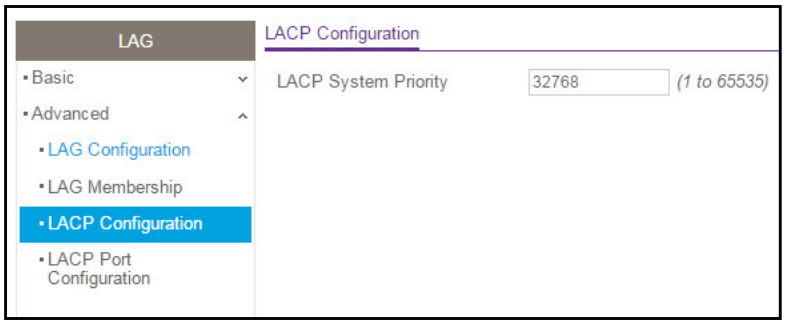
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > LAG > Advanced > LACP Configuration**.



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

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

7. Click the **Apply** button.

   Your settings are saved.

Set the LACP Port Priority Settings

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

To configure LACP port priority settings:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

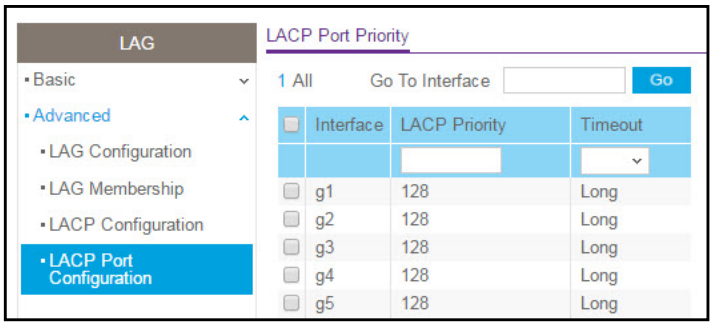
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > LAG > Advanced > LACP Port Configuration**.



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

   This value specifies the interface's link aggregation priority relative to the devices at the other ends of the links on which link aggregation is enabled. A higher value indicates a lower priority. The range is 1 to 65535. The default value is 128.
8. In the **Timeout** field, configure the administrative LACP time-out value:
   - **Long**. Specifies a long time-out value.
   - **Short**. Specifies a short time-out value.
9. Click the **Apply** button.

   Your settings are saved.

Configure VLANs

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

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

Each VLAN in a network is assigned an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station can omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the

packet can either reject it or insert a tag using its default VLAN ID. A port can handle traffic for more than one VLAN, but it can support only one default VLAN ID.

You can define VLAN groups stored in the VLAN membership table. The switch supports up to 64 VLANs.

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

- **VLAN 1**. The default VLAN of which all ports are members.
- **VLAN 2**. The default Auto-VoIP VLAN. By default, this VLAN does not include any members but you can manually add members.
- **VLAN 4089**. The Auto-Video VLAN. By default, this VLAN does not include any members but you can manually add members.

Configure VLAN Settings

You can configure the various VLAN settings.

Add a VLAN

To add a VLAN:

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

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

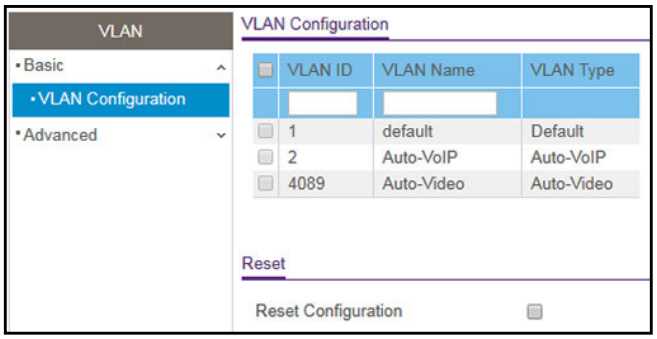
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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 3 to 4093, excluding 4089. (The default VLANs are 1, 2, and 4089).

7. In the **VLAN Name** field, specify a name for the VLAN.

   The VLAN name can be up to 32 alphanumeric characters long, including blanks. You cannot change the names of the default VLANs (that is, the VLANs with ID 1, 2, and 4089).

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

   You cannot change the type of the default VLANs (that is, the VLANs with ID 1, 2, and 4089).

9. Click the **Add** button.

   The VLAN is added to the switch.

Delete a VLAN

To delete a VLAN from the switch:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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 3 to 4093, excluding 4089.

   Note: You cannot delete VLANs 1, 2, and 4089, all of which are predefined.

7. Click the **Delete** button.

   The VLAN is removed.

Reset the VLAN Configuration on the Switch to the Default Settings

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

The VLAN default values are as follows:

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

To reset the VLAN configuration on the switch to the default settings:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

You can also select **Switching > VLAN > Advanced > VLAN Configuration**.

The VLAN Configuration page displays.

6. Select the **Reset Configuration** check box.
7. Click the **Apply** button.

   Your settings are saved. Except for the predefined default VLANs, all VLANs are deleted.

Configure VLAN Membership

To configure VLAN membership:

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

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

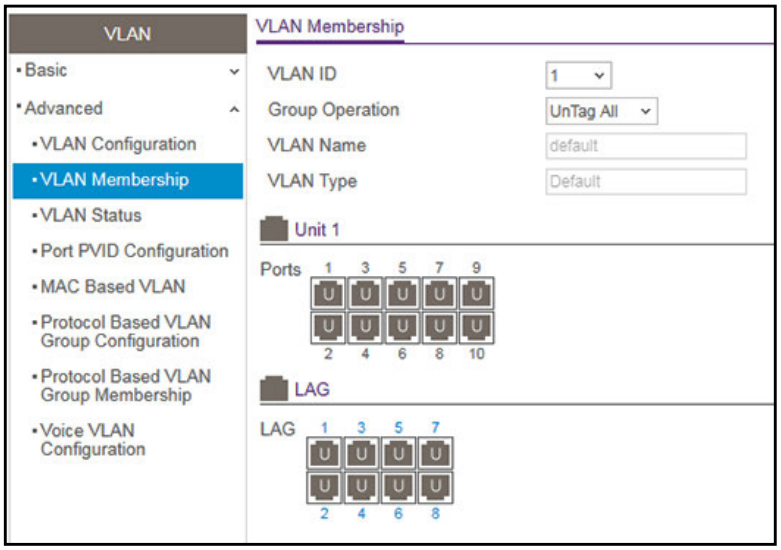
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > VLAN > Advanced > VLAN Membership**.



The previous figure shows the LAG Membership page for model GS310TP.

6. In the **VLAN ID** menu, select the VLAN ID.

   You can select a VLAN that is predefined or that you added (see Add a VLAN on page 112).

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

   By default, the selection is blank and none of the ports are a member of the VLAN. (VLAN 1 is an exception. By default, all ports are untagged members of VLAN 1.)
9. In the LAG table, click each LAG once, twice, or three times to configure one of the following modes or reset the LAG to the default mode:
   - **T (Tagged)**. Selects the LAG as a tagged LAG in the VLAN. All frames transmitted on the LAG are tagged for this VLAN.
   - **U (Untagged)**. Selects the LAG as an untagged LAG in the VLAN. All frames transmitted on the LAG are untagged for this VLAN.
   - **Blank**. The LAG is excluded from the VLAN.

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

    Your settings are saved.

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

Table 22. 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. The names for the following VLANs are predefined: • **VLAN 1**. Default. • **VLAN 2**. Auto-VoIP. • **VLAN 4089**. Auto-Video.
VLAN Type	The type of the VLAN you selected: • **Default** (VLAN ID = 1). Always present. • **Static**. A VLAN that you configured. • **Dynamic**. A dynamically created VLAN.

View the VLAN Status

You can view the status of all currently configured VLANs.

To view the VLAN status:

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

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

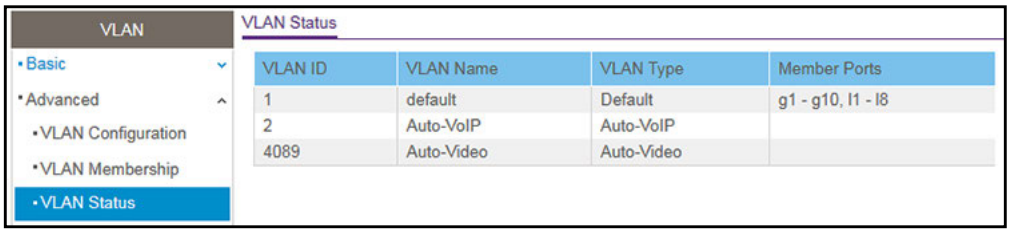
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > VLAN > Advanced > VLAN Status**.



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

Table 23. VLAN status

Field	Definition
VLAN ID	The VLAN identifier (VID) of the VLAN. The range of the VLAN ID is from 1 to 4093.
VLAN Name	The name of the VLAN.
VLAN Type	The VLAN type: • **Default** (VLAN ID = 1). Always present. • **Auto-VoIP** (VLAN ID = 2). Always present. • **Auto-VIdeo** (VLAN ID = 4089). Always present. • **Static**. A VLAN that you configured. • **Dynamic**. A dynamically created VLAN.
Member Ports	The ports, LAGs, or both that are included in the VLAN.

Configure Port PVID Settings

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

- By default, the PVID for each port is 1.
- If you do not specify another value, the default VLAN PVID is used.
- To change the port's default PVID, you must first create a VLAN that includes the port as a member (see Configure VLAN Membership on page 115).

To configure PVID settings:

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

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

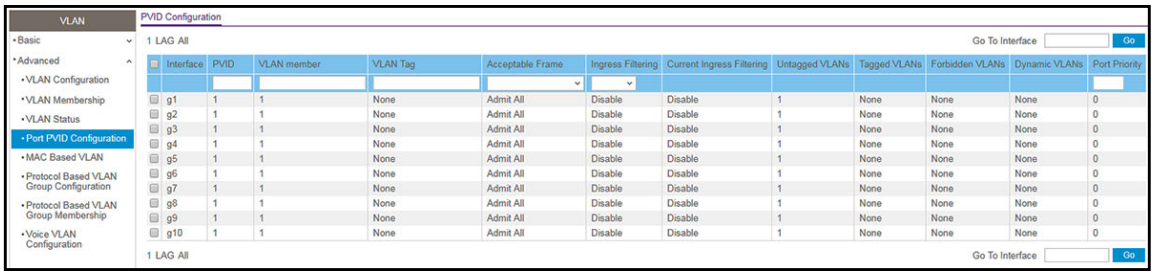
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > VLAN > Advanced > Port PVID Configuration**.



The previous figure shows the PVID Configuration page for model GS310TP.

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 the 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. You can specify port tagging for the VLAN only if the port that you want to add as a tagged port is also member of the VLAN. To reset the VLAN tag configuration to the defaults, use the **None** keyword.
11. From the **Acceptable Frame** menu, specify one if the following types of frames that can be received on the port:
    - **Admit All**. Untagged frames or priority-tagged frames that are received on the port are accepted and assigned the value of the port VLAN ID for the port. This is the default selection.
    - **VLAN Only**. Untagged frames or priority-tagged frames that are received on the port are discarded.
    - **Admit Untagged Only**. Untagged frames that are received on the port are accepted.

    With the **Admit All** and **VLAN Only** selections, VLAN-tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
12. From the **Ingress Filtering** menu, select one of the following options:
    - **Enable**. The frame is discarded if the port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the port VLAN ID specified for the port that received this frame.

- **Disable**. All frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The default is Disable.

13. In the **Port Priority** field, specify the default 802.1p priority assigned to untagged packets arriving at the port.

    You can enter a number from 0 to 7.

14. Click the **Apply** button.

    Your settings are saved.

The following table describes the nonconfigurable fields.

Table 24. Nonconfigurable fields on the PVID Configuration page

Field	Description
Current Ingress Filtering	Indicates 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.
Forbidden VLANs	The number of forbidden VLANs for the interface.
Dynamic VLANs	The number of dynamically added VLANs for the interface.

Configure a MAC-Based VLAN

The MAC-Based VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the source MAC address of the packet.

You define a MAC-to-VLAN mapping by configuring an entry in the MAC-to-VLAN table. An entry is specified through a source MAC address and a VLAN ID. The MAC-to-VLAN configurations are shared across all ports of the switch (that is, a system-wide table exists with MAC address–to–VLAN ID mappings).

When untagged or priority-tagged packets arrive at the switch and entries exist in the MAC-to-VLAN table, the source MAC address of the packet is looked up. If an entry is found, the corresponding VLAN ID is assigned to the packet. If the packet is already priority-tagged, it maintains this value. Otherwise, the priority is set to zero. The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues. Otherwise, the packet is dropped. This implies that you can configure a MAC address mapping to a VLAN that you did not yet create on the switch.

Add a MAC-Based VLAN

To add a MAC-based VLAN:

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

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

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

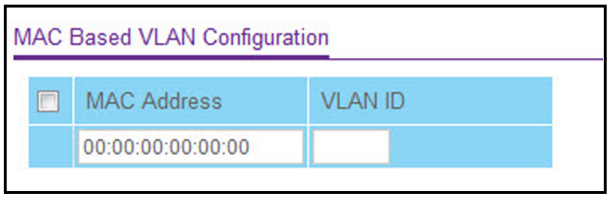
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > VLAN > Advanced > MAC Based VLAN**.



6. In the **MAC Address** field, enter a MAC address to be bound to a VLAN ID.

   This field is configurable only when a MAC-based VLAN is created.
7. In the **VLAN ID** field, specify a VLAN ID in the range from 1 to 4093.
8. Click the **Add** button.

   The MAC address is added to the VLAN mapping.

Delete a MAC Address From VLAN Mapping

To delete a MAC address from VLAN mapping:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

The System Information page displays.

5. Select **Switching > VLAN > Advanced > MAC Based VLAN**.

   The MAC Based VLAN Configuration page displays.

6. In the **MAC Address** field, enter a MAC address.

   This field is configurable only when a MAC-based VLAN exists.

7. In the **VLAN ID** field, specify a VLAN ID in the range from 1 to 4093.
8. Click the **Delete** button.

   The MAC address is removed from the VLAN mapping.

Configure Protocol-Based VLAN Groups

You can use a protocol-based VLAN to define filtering criteria for untagged packets. By default, if you do not configure any port-based (IEEE 802.1Q) or protocol-based VLANs, untagged packets are assigned to VLAN 1. You can override this behavior by defining either port-based VLANs or protocol-based VLANs, or both. Tagged packets are always handled according to the IEEE 802.1Q standard and are not included in protocol-based VLANs.

If you assign a port to a protocol-based VLAN for a specific protocol, untagged frames that arrive on that port for that protocol are assigned the protocol-based VLAN ID. Untagged frames that arrive on the port for other protocols are assigned the port VLAN ID, either the default PVID (1) or a PVID you specifically assigned to the port (see Configure Port PVID Settings on page 118).

You define a protocol-based VLAN by creating a group. Each group forms a one-to-one relationship with a VLAN ID, can include one to three protocol definitions, and can include multiple ports. When you create a group, you specify a name and a group ID is assigned automatically.

To configure a protocol-based VLAN group:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

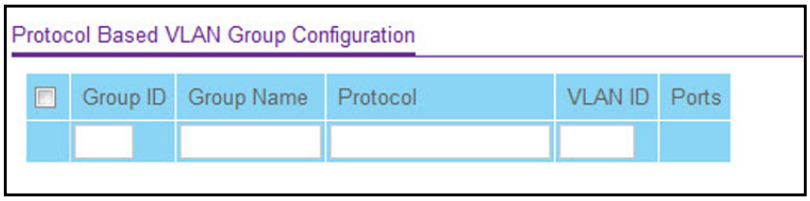
   The login window opens.

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

The default password is **password**.

The System Information page displays.

5. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration**.



6. In the **Group ID** field, enter a number to identify the group.

   The number must be in the range from 1 to 128.

7. In the **Group Name** field, enter a name for the new group.

   You can enter up to 16 characters.

8. In the **Protocol** field, enter one or more protocols that must be associated with the group.

   You can enter keywords such as arp, ip, and ipx. Separate keywords with a comma. You can also enter hexadecimal or decimal values in the range from 0x0600 (1536) to 0xFFFF (65535).

9. In the **VLAN ID** field, enter the VLAN ID.

   The ID can be any number in the range from 1 to 4093. All the ports in the group assign this VLAN ID to untagged packets received for the protocols that you included in this group.

10. Click the **Add** button.

    The protocol-based VLAN group is added to the switch.

    The Ports field displays all the member ports that belong to the group.

Configure Protocol-Based VLAN Group Membership

To configure protocol-based VLAN group membership:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

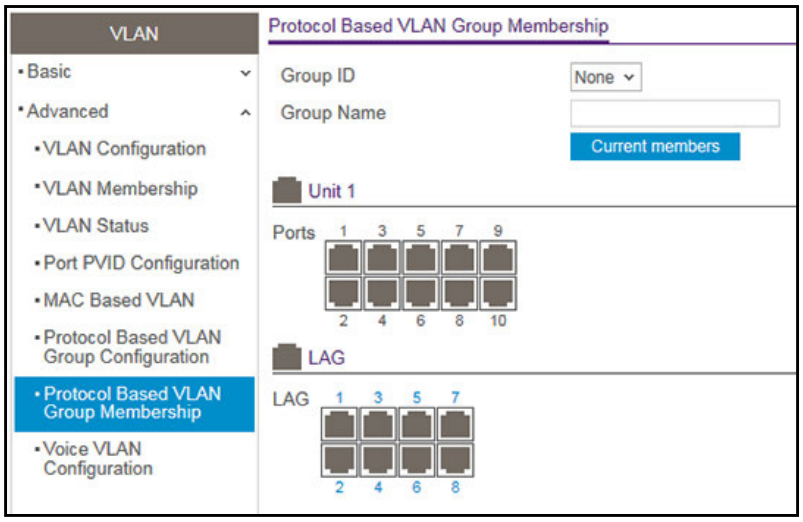
The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Membership**.



   The previous figure shows the Protocol Based VLAN Group Membership page for model GS310TP.

6. From the **Group ID** menu, select the protocol-based VLAN group ID.

   The Group Name field shows the name that is associated with the group.

7. In the Ports table and LAG table, click each port and LAG that you want to include in the protocol-based VLAN group.

   A protocol-based VLAN group can include both port and LAGs. A selected port or LAG is displayed by a check mark.

8. Click the **Apply** button

   Your settings are saved.

9. To display the current numbers in the selected protocol-based VLAN group, click the **Current Members** button.

Configure a Voice VLAN

You can configure the settings for a voice VLAN configuration.

To configure a voice VLAN:

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

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

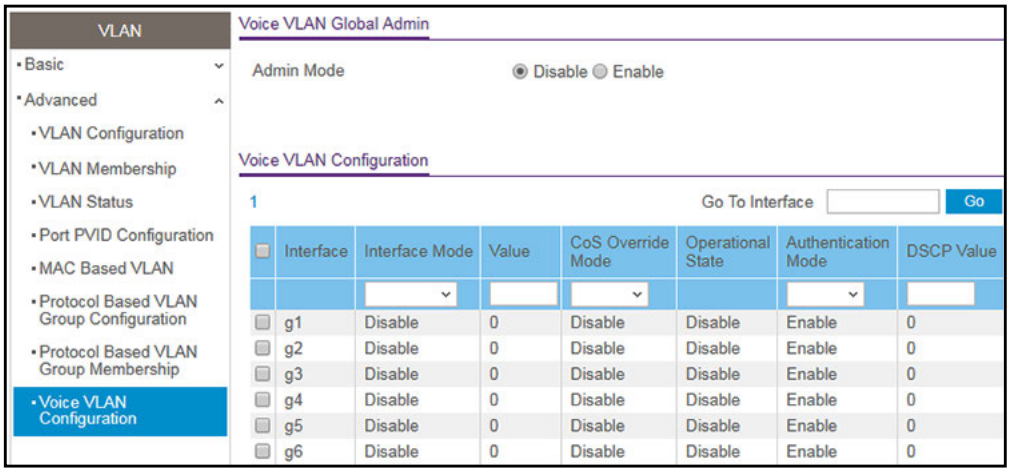
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > VLAN > Advanced > Voice VLAN Configuration**.



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

   This selection specifies the administrative mode for the voice VLAN for the switch. The default is Disable.
7. Select the interface by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.

- To configure multiple interfaces with the same settings, select the check box associated with each interface.
- To configure all interfaces with the same settings, select the check box in the heading row.

8. From the **Interface Mode** menu, select the voice VLAN mode for selected interfaces:
   - **Disable**. This is the default value.
   - **None**. Allow the IP phone to use its own configuration to send untagged voice traffic.
   - **VLAN ID**. Configure the phone to send tagged voice traffic. You must enter the VLAN ID in the **Value** field (see the next step).
   - **Dot1p**. Configure voice VLAN 802.1p priority tagging for voice traffic. You must enter the dot1p value in the **Value** field (see the next step).
   - **Untagged**. Configure the phone to send untagged voice traffic.
9. In the **Value** field, enter the VLAN ID or dot1p value.

   This field is enabled only if you select **VLAN ID** or **Dot1p** from the **Interface Mode** menu.
10. In the **CoS Override Mode** field, select **Disable** or **Enable**.

    The default is Disable.
11. In the **Authentication Mode** field, select **Enable** or **Disable**.

    The default is Enable. When the authentication mode is enabled, voice traffic is allowed on an unauthorized voice VLAN port. When the authentication mode is disabled, devices are authorized through dot1x.

    Note: Authentication through dot1x is possible only if dot1x is enabled.
12. In the **DSCP Value** field, configure the Voice VLAN DSCP value for the port.

    The range is from 0 to 64. The default value is 0.
13. Click the **Apply** button.

    Your settings are saved.

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

Configure Auto-VoIP

Voice over Internet Protocol (VoIP) enables telephone calls over a data network. Because voice traffic is typically more time-sensitive than data traffic, the Auto-VoIP feature provides a classification for voice packets so that they can be prioritized above data packets, allowing the switch to provide better Quality of Service (QoS). With the Auto-VoIP feature, voice prioritization is provided based on the SIP call-control protocol or OUI bits.

Configure Protocol-Based Port Settings for VoIP

To prioritize time-sensitive voice traffic over data traffic, protocol-based Auto-VoIP checks for packets carrying the Session Initiation Protocol (SIP) VoIP protocol.

VoIP frames that are received on ports that for which the Auto-VoIP feature is enabled are marked with the specified CoS traffic class value.

To configure protocol-based port settings for VoIP:

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

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

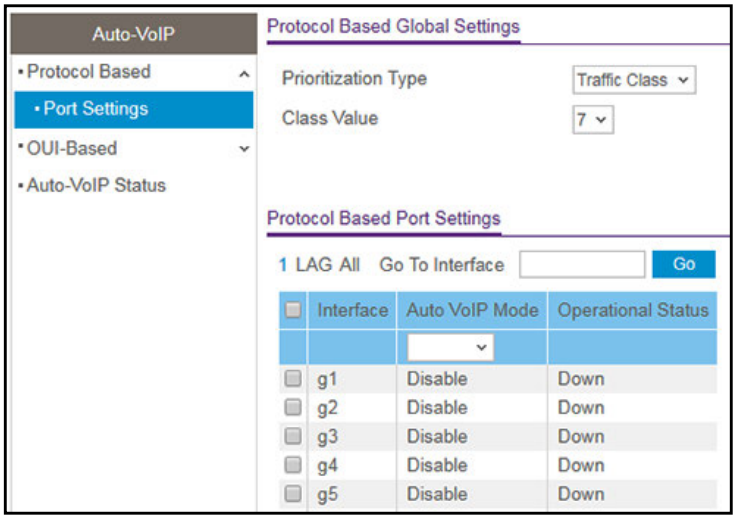
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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**.



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

   This selection specifies the type of prioritization.

7. From the **Class Value** menu, specify the CoS class value to be reassigned for packets that the voice VLAN receives.
8. Click the **Apply** button.

   Your settings are saved.

Configure Auto-VoIP OUI-Based Properties

With Organizationally Unique Identifier (OUI)–based Auto-VoIP, voice prioritization is provided based on OUI bits.

To configure Auto-VoIP OUI-based properties:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Auto-VoIP > OUI-based > Properties**.

   The OUI-Based Properties page displays.
6. In the **Auto-VoIP VLAN ID** field, enter the VoIP VLAN ID of the switch.

   The default Auto-VoIP VLAN ID is 2. You can use that VLAN ID or create another VLAN ID for Auto-VoIP.
7. From the **OUI-based priority** menu, select the OUI-based priority of the switch, from 0 to 7.

   The default value is 7.
8. Click the **Apply** button.

   Your settings are saved.

Configure the OUI-Based Port Settings

You can configure the OUI port settings.

To configure OUI-based port settings:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

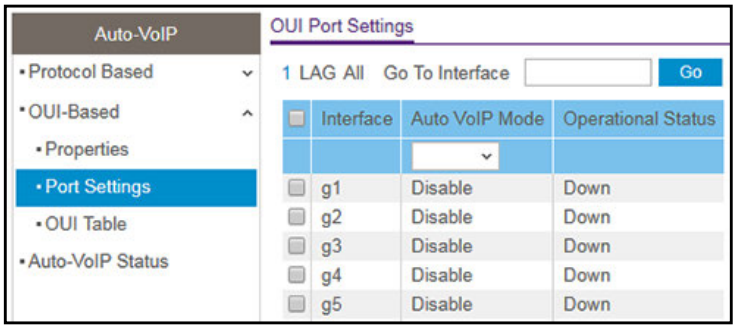
   The login window opens.

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.

8. Click the **Apply** button.

   Your settings are saved.

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

Manage the OUI Table

Device hardware manufacturers can include an OUI in a network adapter to help identify a hardware device. The OUI is a unique 24-bit number assigned by the IEEE registration authority. The switch comes preconfigured with the following OUIs that identify the IP phone manufacturer:

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

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

Configure the OUI Table

To configure the OUI Table:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Auto-VoIP > OUI-based > OUI Table**.

   The OUI Table page displays.

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

   You can configure up to 32 OUIs.

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

   The maximum length of description is 32 characters.

8. Click the **Add** button.

   The telephony OUI entry is added.

Delete One or More OUI Prefixes From the OUI Table

To delete one or more OUI prefixes from the OUI table:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Auto-VoIP > OUI-based > OUI Table**.

   The OUI Table page displays.

6. Select the check box next to each OUI prefix to be removed.
7. Click the **Delete** button.

   The telephony OUI entries are removed.

Display the Auto-VoIP Status

You can display the Auto-VoIP status.

To view the Auto-VoIP status:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Auto-VoIP > Auto-VoIP Status**.

   The Auto-VoIP Status page displays.
6. To refresh the page with the latest information about the switch, click the **Update** button.

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

Table 25. Auto-VoIP status

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 network devices. STP also provides one path between end stations on a network, eliminating loops. STP (also referred to as “classic” STP) provides a single path between end stations, avoiding and eliminating loops. For information about configuring the global STP settings for the switch, see Configure the STP Settings and View the STP Status on page 133.

The switch support the following spanning tree versions:

- **CST**. Common STP. For information on configuring CST, see Configure and View the CST Settings on page 135 and Configure and View the CST Port Settings on page 137.
- **MSTP**. Multiple Spanning Tree Protocol (MSTP, also referred to as MST) supports multiple instances of spanning tree to efficiently channel VLAN traffic over different interfaces. For information on configuring MSTP, see Manage MST Settings on page 142 and Configure and View the Port Settings for an MST Instance on page 144.
- **RSTP**. Rapid STP. Each instance of the spanning tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree (RSTP), with slight modifications in the working but not the end effect (chief among the effects is the rapid transitioning of the port to the forwarding state). For information on viewing the RSTP state, see View Rapid STP Information on page 141.

  The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full-duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to the forwarding state and the suppression of Topology Change Notification. These features are represented by the parameters pointtopoint and edgeport. MSTP is compatible with both RSTP and STP. It behaves in a way that is appropriate for STP and RSTP bridges. An MSTP bridge can be configured to behave entirely as an RSTP bridge or an STP bridge.

Note: For two bridges to be in the same region, the force version must be 802.1s and their configuration names, digest keys, and revision levels must match. For additional information about regions and their effect on network topology, refer to the IEEE 802.1Q standard.

Configure the STP Settings and View the STP Status

You can configure the STP settings and view the STP status on the switch.

To configure the STP settings and view the STP status:

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

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

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

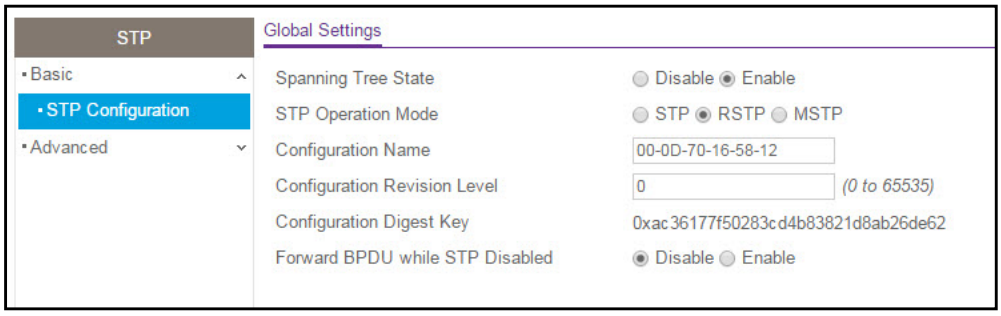
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > STP > Basic > STP Configuration**.



6. Configure the following global settings for the switch:
   a. **Spanning Tree State**. Enable or disable the spanning tree operation on the switch.

      By default, spanning tree operation is disabled.

   b. **STP Operation Mode**. Specify the STP version for the switch.

      The options are **STP**, **RSTP**, and **MSTP**. The default is RSTP.

   c. **Configuration Name**. Specify a name to identify the STP, RSTP, or MSTP configuration.

      The name can be up to 32 alphanumeric characters.

   d. **Configuration Revision Level**. Specify an identifier to identify the STP, RSTP, or MSTP configuration.

      The values can be from 0 to 65535. The default value is 0.

   e. **Forward BPDU while STP Disabled**. Enable or disable the bridge protocol data unit (BPDU) flood.

      This setting specifies whether spanning tree BPDUs are forwarded while spanning tree is disabled on the switch.
7. Click the **Apply** button.

   Your settings are saved.

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

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

Table 26. STP Configuration status

Field	Description
Global Settings	
Configuration Digest Key	The identifier used to identify the configuration currently being used.
STP Status	
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 setting for the switch that indicates if a topology change is in progress on any port assigned to the CST. The option is True or False.
Designated Root	The bridge identifier of the root bridge. It consists of the bridge priority and the base MAC address of the bridge.
Root Path Cost	The path cost to the designated root for the CST.
Root Port	The 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 setting.
Hold Time (secs)	The minimum time in seconds between the transmission of configuration BPDUs.
CST Regional Root	The priority and base MAC address of the CST regional root.
CST Path Cost	The path cost to the CST tree regional root.

Configure and View the CST Settings

You can configure a common spanning tree (CST) and internal spanning tree on the switch.

To configure and view the CST settings:

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

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

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

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

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

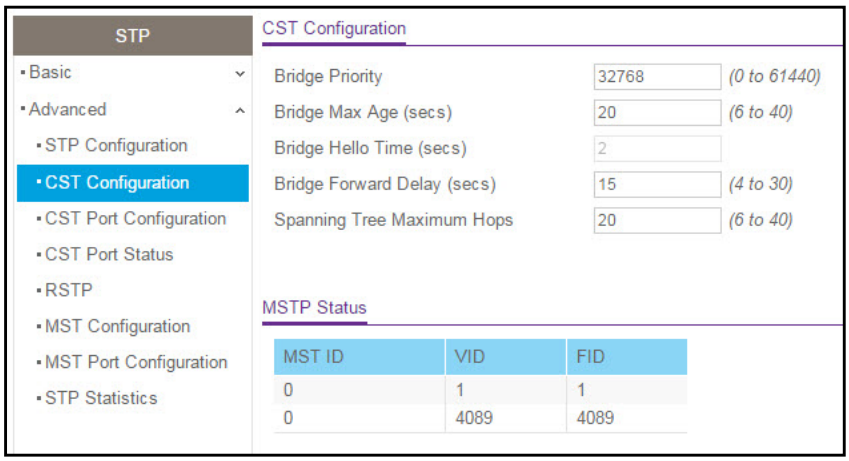
The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > STP > Advanced > CST Configuration**.



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

forwarding packets. The value must be greater or equal to (Bridge Max Age / 2) + 1. The time range is from 4 seconds to 30 seconds. The default value is 15 seconds.

- **Spanning Tree Maximum Hops**. The maximum number of bridge hops the information for a particular CST instance can travel before being discarded. The range is from 6 to 40. The default is 20 hops.

7. Click the **Apply** button.

   Your settings are saved.

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

The following table describes the MSTP Status information that is displayed.

Table 27. STP advanced CST configuration, MSTP status

Field	Description
MST ID	The MST instances (including the CST) and the corresponding VLAN IDs associated with each of them.
VID ID	The VLAN IDs and the corresponding FID associated with each of them.
FID ID	The FIDs and the corresponding VLAN IDs associated with each of them.

Configure and View the CST Port Settings

You can configure a common spanning tree (CST) and internal spanning tree on a specific port on the switch.

A port can become diagnostically disabled (D-Disable) when DOT1S experiences a severe error condition. The most common cause is when the DOT1S software experiences BPDU flooding. The flooding criteria are such that DOT1S receives more than 15 BPDUs in a 3-second interval. The other causes for DOT1S D-Disable are very rare.

To configure and view the CST port settings:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

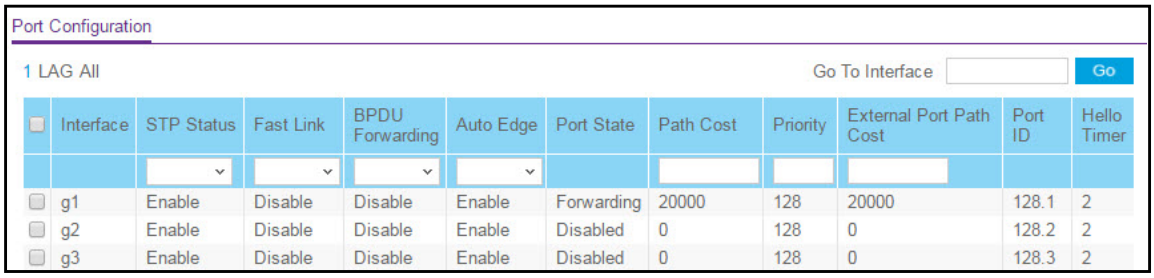
   The login window opens.

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

The default password is **password**.

The System Information page displays.

5. Select **Switching > STP > Advanced > CST Port Configuration**.



6. Select 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 **STP Status** menu, select the option to enable or disable the spanning tree administrative mode associated with the port or LAG.

   The option is **Enable** or **Disable**. The default value is Enable.
8. From the **Fast Link** menu, select whether the specified port is an edge port within the CST.

   The option is **Enable** or **Disable**. The default value is Disable.
9. From the **BPDU Forwarding** menu, configure BPDU forwarding.

   The option is **Enable** or **Disable**. The default value is Disable. When BPDU forwarding is enabled, the switch forwards the BPDU traffic arriving on the port when STP is disabled on the port.
10. From the **Auto Edge** menu, specify if the port is allowed to become an edge port if it does not detect BPDUs for some time.

    The option is **Enable** or **Disable**. The default value is Enable.
11. In the **Path Cost** field, set the path cost to a new value for the specified port in the common and internal spanning tree.

    Specify a value in the range from 0 to 200000000. The default is 0. When the path cost is set to 0, the value is updated with the external path cost from an incoming STP packet.
12. 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 value is 128.

13. In the **External Port Path Cost** field, set the external path cost to a new value for the specified port in the spanning tree.

    The value range is 0 to 200000000. The default is 0.

14. Click the **Apply** button.

    Your settings are saved.

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

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

Table 28. CST port configuration

Field	Description
Port State	The forwarding state of the 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 setting for the CST. The default is 2 seconds.

View the CST Port Status

You can display the common spanning tree (CST) and internal spanning tree for a specific port on the switch.

To view the CST port status:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

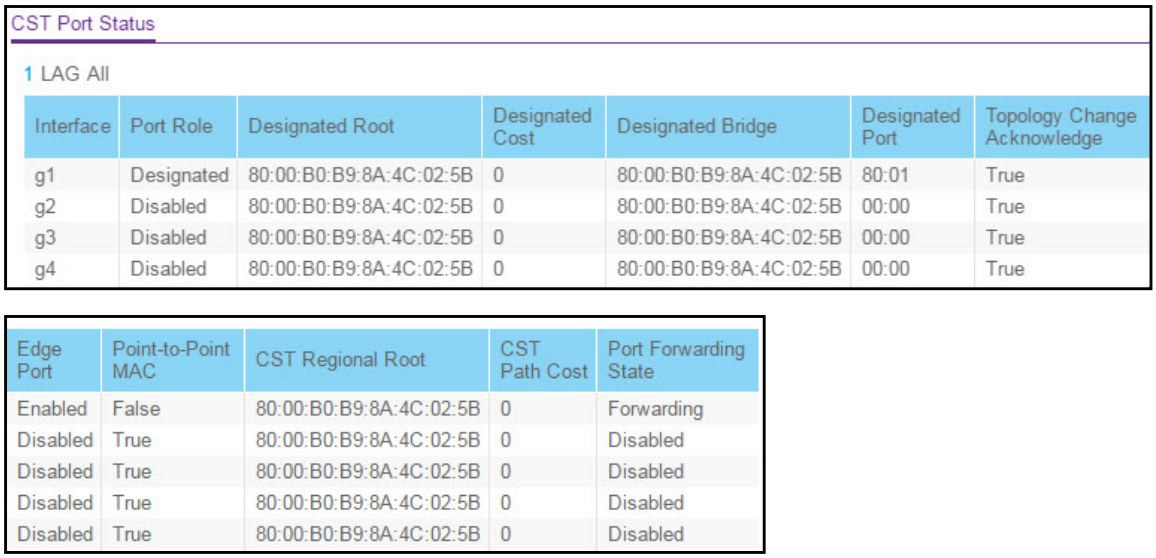
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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



CST Port Status

1 LAG All

Interface	Port Role	Designated Root	Designated Cost	Designated Bridge	Designated Port	Topology Change Acknowledge
g1	Designated	80:00:B0:B9:8A:4C:02:5B	0	80:00:B0:B9:8A:4C:02:5B	80:01	True
g2	Disabled	80:00:B0:B9:8A:4C:02:5B	0	80:00:B0:B9:8A:4C:02:5B	00:00	True
g3	Disabled	80:00:B0:B9:8A:4C:02:5B	0	80:00:B0:B9:8A:4C:02:5B	00:00	True
g4	Disabled	80:00:B0:B9:8A:4C:02:5B	0	80:00:B0:B9:8A:4C:02:5B	00:00	True

Edge Port	Point-to-Point MAC	CST Regional Root	CST Path Cost	Port Forwarding State
Enabled	False	80:00:B0:B9:8A:4C:02:5B	0	Forwarding
Disabled	True	80:00:B0:B9:8A:4C:02:5B	0	Disabled
Disabled	True	80:00:B0:B9:8A:4C:02:5B	0	Disabled
Disabled	True	80:00:B0:B9:8A:4C:02:5B	0	Disabled
Disabled	True	80:00:B0:B9:8A:4C:02:5B	0	Disabled

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

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

Table 29. CST port status

Field	Description
Interface	The physical port or LAG that is 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 can be Root, Designated, Alternate, Backup, Master, or Disabled.
Designated Root	The root bridge for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	The path cost offered to the LAN by the designated port.
Designated Bridge	The identifier of the bridge with the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	The port identifier on the designated bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.
Topology Change Acknowledge	Identifies whether the topology change acknowledgement flag is set for the next BPDU to be transmitted for the port. It is either True or False.
Edge port	Indicates whether the port is enabled as an edge port. It is either Enabled or Disabled.
Point-to-point MAC	The derived value of the point-to-point status.
CST Regional Root	The 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	The path cost to the CST regional root.
Port Forwarding State	The forwarding state of the port.

View Rapid STP Information

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

To view information about RSTP:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > STP > Advanced > RSTP**.
6. To refresh the page with the latest information about the switch, click the **Update** button.

The following table describes the Rapid STP Status information displayed on the page.

Table 30. 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 can be Root, Designated, Alternate, Backup Master, or Disabled.
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 the port.

Manage MST Settings

You can configure a multiple spanning tree (MST) on the switch.

Configure an MST Instance

To configure an MST instance:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

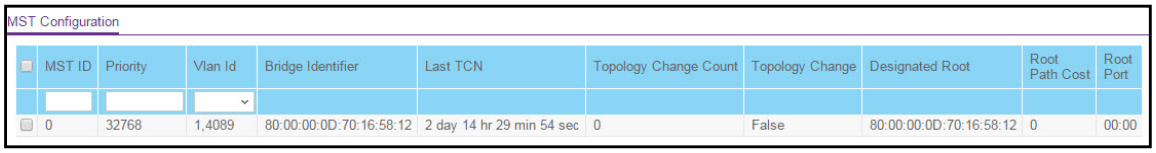
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > STP > Advanced > MST Configuration**.



6. Configure the MST values:
   - **MST ID**. Specify the ID of the MST to create. The range is from 1 to 4094. This is visible only when the select option of the MST ID select box is selected.
   - **Priority**. The bridge priority value for the MST. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if you set the priority to any value between 0 and 4095, the switch automatically sets the value to 0. The default value is 32768. The range is from 0 to 61440.
   - **VLAN Id**. The menu includes all VLANs that are configured on the switch. You can select VLANs that must be associated with the MST instance or clear VLANs that are already associated with the MST instance.
7. Click the **Add** button.

The MST is added.

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

Table 31. 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 the format “day:hour:minute:second” since the topology of the selected MST instance last changed.
Topology Change Count	The number of times that the topology changed for the selected MST instance.
Topology Change	The value of the topology change settings for the switch, indicating if a topology change is in progress on any port assigned to the selected MST instance. It is either True or False.
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	The path cost to the designated root for this MST instance.
Root Port	The 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 Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch’s password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > STP > Advanced > MST Configuration**.

   The MST Configuration page displays.
6. Select the check box next to the instance.

You can select multiple check boxes to apply the same setting to all selected ports.

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

   Your settings are saved.

Delete an MST Instance

To delete an MST instance:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > STP > Advanced > MST Configuration**.

   The MST Configuration page displays.
6. Select the check box for the instance.
7. Click the **Delete** button.

   The MST instance is removed.

Configure and View the Port Settings for an MST Instance

You can configure and display the Multiple Spanning Tree (MST) settings on a specific port on the switch.

A port can become diagnostically disabled (D-Disable) when DOT1S experiences a severe error condition. The most common cause is when the DOT1S software experiences BPDU flooding. The flooding criteria is such that DOT1S receives more than 15 BPDUs in a 3-second interval. The other causes for DOT1S D-Disable are extremely rare.

To configure and view the port settings for an MST instance:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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 MST Port Configuration page displays.

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

6. From the **Select MST** menu, select the MST instance.

   You can select only instances that you added to the switch (see Manage MST Settings on page 142).

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. Configure the MST values for the selected interfaces:
   - **Port Priority**. The priority for a particular port within the selected MST instance. The port priority is set in multiples of 16. If you specify a value that is not a multiple of 16, the priority is set to the 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 from 0 to 240.
   - **Port Path Cost**. Set the path cost to a new value for the specified port in the selected MST instance. Specify a value in the range from 0 to 200000000.

9. Click the **Apply** button.

Your settings are saved.

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

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

Table 32. MST port status information

Field	Description
Auto Calculated Port Path Cost	Indicates whether the path cost is automatically calculated (Enabled) or not (Disabled). Path cost is calculated based on the link speed of the port if the configured value for Port Path Cost is zero.
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	The time since the counters were last cleared, displayed in days, hours, minutes, and seconds.
Port Mode	The Spanning Tree Protocol administrative mode that is associated with the port or port channel. The option is Enable or Disable.
Port Forwarding State	The current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. The options are as follows: • **Disabled**. STP is currently disabled on the port. The port forwards traffic while learning MAC addresses. • **Discarding**. The port is currently blocked. The port cannot forward traffic nor can it learn MAC addresses. • **Manual Forwarding**. STP is currently disabled on the port. The port forwards traffic while learning 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 can be Root, Designated, Alternate, Backup, Master, or Disabled.
Designated Root	The 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	The cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
Designated Bridge	The 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	The port identifier on the designated bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.

View the 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 the spanning tree statistics:

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

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

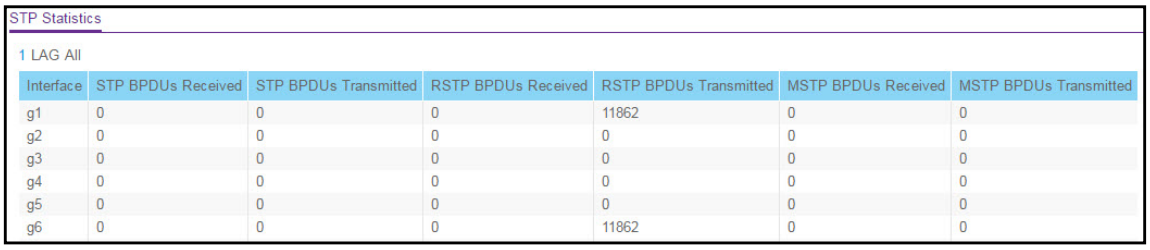
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > STP > Advanced > STP Statistics**.



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

The following table describes the information available about the STP Statistics page.

Table 33. STP Statistics

Field	Description
Interface	The physical port or LAG on the switch.
STP BPDUs Received	The number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	The number of STP BPDUs transmitted from the selected port.
RSTP BPDUs Received	The number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	The number of RSTP BPDUs transmitted from the selected port.

Table 33. STP Statistics (continued)

Field	Description
MSTP BPDUs Received	The number of MSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	The 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.

View and Search the MFDB Table

The Multicast Forwarding Database (MFDB) holds the port membership information for all active multicast address entries. The key for an entry consists of a VLAN ID and MAC address pair. Entries can contain data for more than one protocol.

To view and search the MFDB Table:

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

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

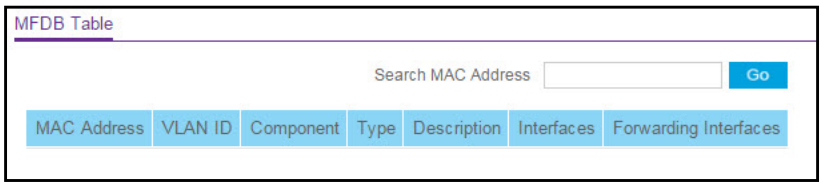
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Multicast > MFDB > MFDB Table**.



6. In the **Search by MAC Address** field, enter a MAC address.

   Enter six two-digit hexadecimal numbers separated by colons, for example 00:01:23:43:45:67.

7. Click the **Go** button.

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

8. To refresh the page with the latest information about the switch, click the **Update** button.
9. To clear all multicast forwarding address entries, click the **Clear** button.

Table 34. 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	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	The component that is responsible for this entry in the Multicast Forwarding Database. The options are IGMP snooping, GMRP, Static Filtering, and MLD snooping.
Description	The text description of this multicast table entry. The options are Management Configured, Network Configured, and Network Assisted.
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 Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > MFDB > MFDB Statistics**.

   The MFDP Statistics page displays.

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

The following table describes the MFDB Statistics fields.

Table 35. MFDB Statistics information

Field	Description
Max MFDB Table Entries	The maximum number of entries that the Multicast Forwarding Database table can hold (256 entries).
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.

Configure the Auto-Video Multicast Settings

You can configure the auto-video multicast settings.

To configure auto-video multicast settings:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > Auto-Video**.

   The Auto-Video Configuration page displays.

6. Select one of the following radio buttons:
   - Select the **Disable** radio button to globally disable Auto-Video administrative mode for the switch.

- Select the **Enable** radio button to globally enable Auto-Video administrative mode for the switch.

7. Click the **Apply** button.

   Your settings are saved.

   The Auto-Video VLAN field displays the Auto-Video VLAN ID that is configured on the switch. By default, this VLAN ID is 4089.

About IGMP Snooping

Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward multicast traffic intelligently. Multicast 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 detected or processed by all connected nodes. For multicast packets, this approach could lead to a less efficient use of the network bandwidth, particularly when the packets are intended for a small number of nodes only. Packets are flooded into network segments where no node is receptive to the packet. Although nodes rarely incur any processing overhead to filter packets addressed to unrequested group addresses, the nodes cannot transmit new packets onto the shared media while the multicast packets are being flooded. Such as waste of bandwidth is even worse when the LAN segment is not shared, for example in full-duplex links.

Allowing switches to snoop IGMP packets can solve this problem. While the IGMP packets are being forwarded throughout the network, the switch uses the information in the packets to determine which segments must receive packets that are directed to the group address.

Configure IGMP Snooping

You can configure the settings for IGMP snooping, which is used to build forwarding lists for multicast traffic.

To configure IGMP snooping:

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

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

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

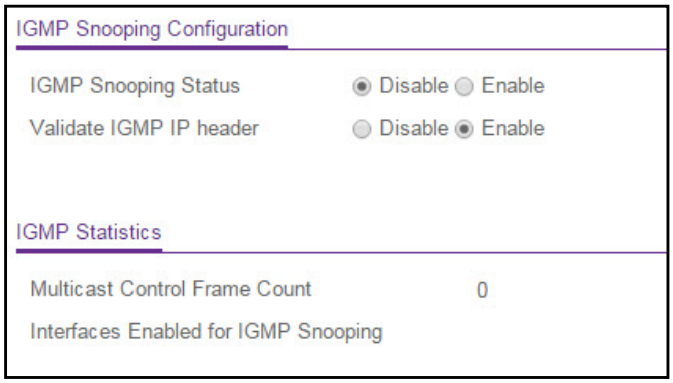
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Multicast > IGMP Snooping > Configuration**.



6. Select the IGMP Snooping Status **Enable** or **Disable** radio button.

   This specifies the administrative mode for IGMP snooping for the switch. The default is Disable.
7. Select the Validate IGMP IP header **Enable** or **Disable** radio button.

   When IGMP IP header validation is enabled, any IGMP IP header must include the Router Alert, ToS, and TTL information. Otherwise, the IGMP packet is discarded. The default value is Enable.
8. Click the **Apply** button.

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

The following table displays information about the global IGMP snooping status and statistics on the page.

Table 36. 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	The interfaces that are enabled for IGMP snooping.
VLAN IDs Enabled For IGMP Snooping	The IDs of the VLANs that are enabled for IGMP snooping.
VLAN IDs Enabled For IGMP Snooping Querier	The IDs of the VLANs that are 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.

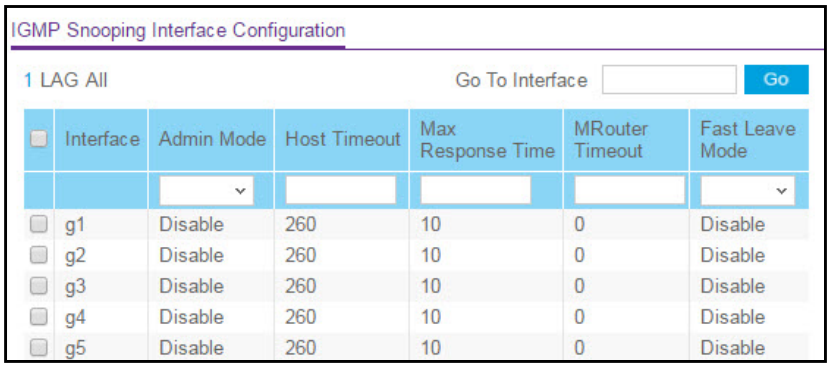
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Multicast > IGMP Snooping > Interface Configuration**.



6. Select 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 1 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 greater or equal to 1 and less than the group membership interval in seconds. The default is 10 seconds. The configured value must be less than the group membership interval.
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 option are **Enable** and **Disable**. The default is Disable.
12. Click the **Apply** button.

    Your settings are saved.

View, Search, or Clear the IGMP Snooping Table

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

To view, search, or clear the IGMP snooping table:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping Table**.

   The IGMP Snooping Table page displays.
6. In the **Search By MAC Address** field, specify the MAC address whose MFDB table entry you want to view.

   Enter six two-digit hexadecimal numbers separated by colons, for example 00:01:23:43:45:67.
7. Click the **Go** button.

   If the address exists, the entry is displayed. An exact match is required.
8. To refresh the page with the latest information about the switch, click the **Update** button.
9. To clear all multicast forwarding address entries that were created for IGMP snooping, click the **Clear** button.

The following table describes the information in the IGMP snooping table.

Table 37. IGMP Snooping Table information

Field	Description
MAC Address	The multicast MAC address for which the switch holds forwarding and/or filtering information. The format is six two-digit hexadecimal numbers that are separated by colons, for example, 01:00:5e:45:67:89.
VLAN ID	The VLAN ID for which the switch holds forwarding and filtering information.

Table 37. IGMP Snooping Table information (continued)

Field	Description
Type	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.
Description	The text description of this multicast table entry. The options are Management Configured, Network Configured, and Network Assisted.
Interface	The 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.

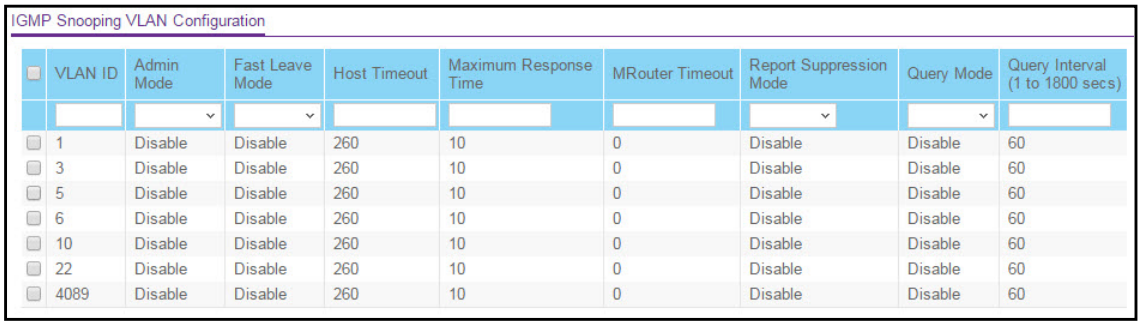
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping VLAN Configuration**.



6. Select the check boxes for one or more VLANs.

   If you select the check box for a single VLAN, the VLAN ID displays in the VLAN ID field.

7. Configure the IGMP snooping values for the selected VLAN or VLANs:
   - **Admin Mode**. Enable or disable IGMP snooping for the specified VLAN ID. The default is Disable.
   - **Fast Leave Mode**. Enable or disable the IGMP snooping fast leave mode for the specified VLAN ID. The default is Disable.
   - **Host Timeout**. Set the value for group membership interval of IGMP snooping for the specified VLAN ID. The range is from the value for the Maximum Response Time plus 1 to 3600 seconds. The default is 260 seconds.
   - **Maximum Response Time**. Set the value for the maximum response time of IGMP snooping for the specified VLAN ID. The range is from 1 to the Host Timeout value minus 1. This value must be greater than group membership interval value. The default is 10 seconds.
   - **MRouter Timeout**. Set the value for multicast router expiry time of IGMP snooping for the specified VLAN ID. The range is from 0 to 3600 seconds. The default is 0 seconds.
   - **Report Suppression Mode**. Enable or disable IGMP snooping report suppression mode for the specified VLAN ID. IGMP snooping report suppression allows the suppression of the IGMP reports sent by the multicast hosts by building a Layer 3 membership table. The results is that only the most essential reports are sent to the IGMP routers so that the routers can continue to receive the multicast traffic.The default is Disable.
   - **Querier Mode**. Enable or disable the IGMP querier mode. The default is Disable.
   - **Query Interval**. Set the IGMP query interval for the specified VLAN ID. The range is from 1 to 1800 seconds. The default is 60 seconds.
8. Click the **Apply** button.

   Your settings are saved.

Modify IGMP Snooping Settings for a VLAN

To modify IGMP snooping settings for a VLAN:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping VLAN Configuration**.

   The IGMP Snooping VLAN Configuration page displays.
6. Select the check box next to the VLAN ID.
7. Update the values.
8. Click the **Apply** button.

   Your settings are saved.

Disable IGMP Snooping on a VLAN

To disable IGMP snooping on a VLAN:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping VLAN Configuration**.

   The IGMP Snooping VLAN Configuration page displays.
6. Select the check box next to the VLAN ID.
7. From the **Admin Mode** menu, select **Disable**.
8. Click the **Apply** button.

   Your settings are saved.

Configure a Multicast Router Interface

You can configure an interface as the designated interface to which a multicast router is connected. All IGMP packets snooped by the switch are forwarded to the multicast router reachable from the interface. Configuring a multicast router interface is usually not required because the switch automatically detects the multicast router and forwards IGMP packets accordingly. This configuration is required only if you want to make sure that the multicast router always receives IGMP packets from the switch in a complex network.

To configure a multicast router interface:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

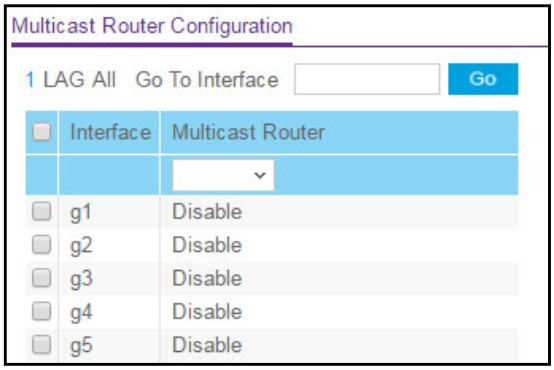
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > IGMP Snooping > Multicast Router Configuration**.



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 **Multicast Router** menu, select **Enable** or **Disable**.
8. Click the **Apply** button.

   Your settings are saved.

Configure a Multicast Router VLAN

You can configure an interface to forward only snooped IGMP packets from a specific VLAN to the multicast router connected to the interface. This configuration is usually not required because the switch automatically detects a multicast router and forwards the IGMP packets accordingly. This configuration is required only if you want to make sure that the multicast router always receives IGMP packets from the switch in a complex network.

To configure a multicast router VLAN:

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

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

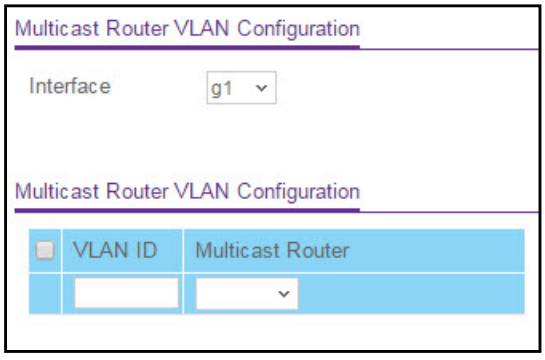
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Multicast > IGMP Snooping > Multicast Router VLAN Configuration**.



6. From the **Interface** menu, select the interface.

7. In the **VLAN ID** field, enter the VLAN ID.
8. From the **Multicast Router** menu, select **Enable** or **Disable**.
9. Click the **Apply** button.

   Your settings are saved.

IGMP Snooping Querier Overview

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

You can configure and display information about IGMP snooping queriers on the network and, separately, on VLANs.

Configure an IGMP Snooping Querier

You can configure the settings for an IGMP snooping querier.

To configure the settings for an IGMP snooping querier:

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

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

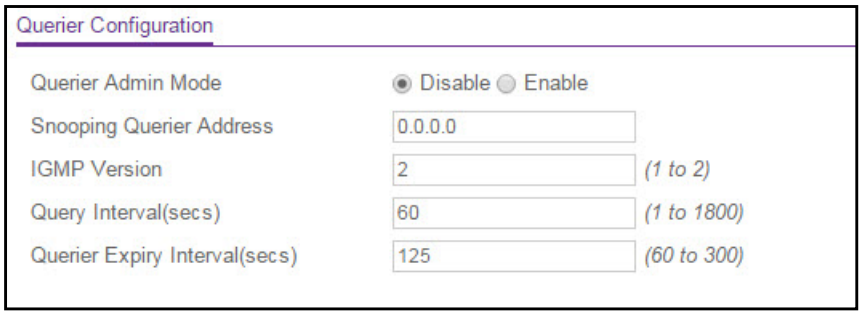
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Multicast > IGMP Snooping Querier > Querier Configuration**.



6. Configure the following settings:
   - **Querier Admin Mode**. Enable or disable IGMP snooping for the switch. The default is Disable.
   - **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 value is 2.
   - **Query Interval(secs)**. Specify the time interval in seconds between periodic queries sent by the snooping querier. The query interval must be in the range from 1 to 1800. The default value is 60 seconds.
   - **Querier Expiry Interval(secs)**. Specify the time interval in seconds after which the last querier information is removed. The querier expiry interval must be in the range from 60 to 300. The default value is 125 seconds.
7. Click the **Apply** button.

   Your settings are saved.

Configure an IGMP Snooping Querier for VLANs

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

To configure IGMP snooping for a VLAN ID:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

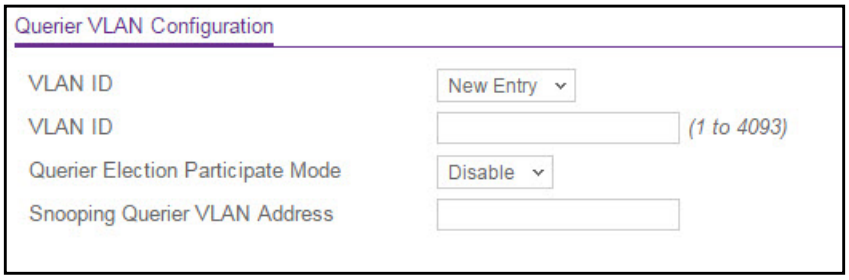
The login window opens.

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 must be enabled. You can select an existing VLAN only.
   - **Querier Election Participate Mode**. Enable or disable the querier mode:
     - **Disable**. Upon seeing another querier of the same version in the VLAN, the snooping querier moves to the non-querier state.
     - **Enable**. The snooping querier participates in querier election, in which the lowest IP address operates as the querier in that VLAN. The other querier moves to non-querier state.
   - **Snooping Querier VLAN Address**. Specify the snooping querier IP address to be used as the source address in periodic IGMP queries that are sent to the VLAN.
8. Click the **Apply** button.

   Your settings are saved.

Display IGMP Snooping Querier for VLAN Status

To display querier VLAN status:

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

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

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

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

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

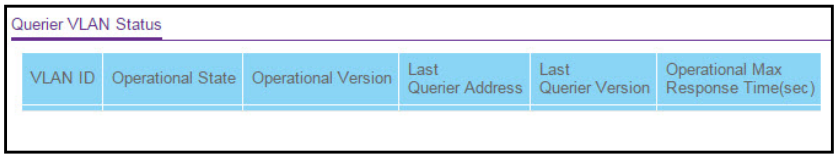
The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Status**.



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

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

Table 38. 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: • **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	The maximum response time to be used in the queries that are sent by the snooping querier.

View, Search, and Manage the MAC Address Table

You can view or configure the MAC Address Table. This table contains information about unicast entries for which the switch holds forwarding or filtering information. This information lets the transparent bridging function determine how an incoming frame must be propagated.

If you clear the MAC address entries in the MAC Address Table, only the dynamic entries are removed.

View, Search, or Clear the MAC Address Table

To view, search, or clear the MAC Address Table:

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

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

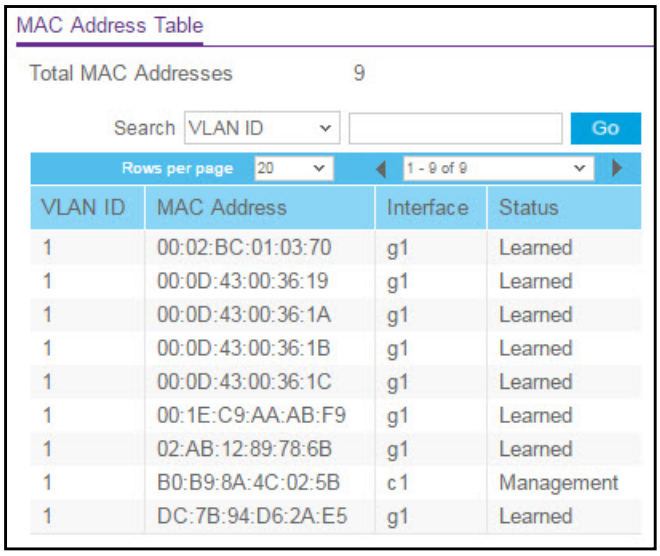
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Address Table > Basic > Address Table**.



6. Use the **Search** menu and field to search for a MAC address, VLAN ID, or interface number:
   - **Search by MAC Address**. From the **Search** menu, select **MAC Address**, and enter the 6-byte hexadecimal MAC address in two-digit groups separated by colons, for example, 01:23:45:67:89:AB. Then click the **Go** button.

     If the address exists, that entry is displayed as the first entry followed by the remaining (higher) MAC addresses. An exact match is required.
   - **Search VLAN ID**. From the **Search** menu, select **VLAN ID**, and enter the VLAN ID, for example, 100. Then click the **Go** button.
   - **Search Interface**. From the **Search** menu, select **Interface**, and enter the interface ID using the respective interface naming convention (for example, g1 or l1). Then click the **Go** button.
7. To refresh the page with the latest information about the switch, click the **Update** button.
8. To clear all dynamic MAC address entries in the table, click the **Clear** button.

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

Table 39. MAC Address Table information

Field	Description
Total MAC Address	The number of MAC addresses learned or configured.
VLAN ID	The VLAN ID associated with the MAC address.
MAC Address	The unicast MAC address for which the switch holds forwarding and/or filtering information. The format is a 6-byte MAC address that is separated by colons, for example 01:23:45:67:89:AB.

Table 39. 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: • **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 forwarding database.

To set the address aging interval:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

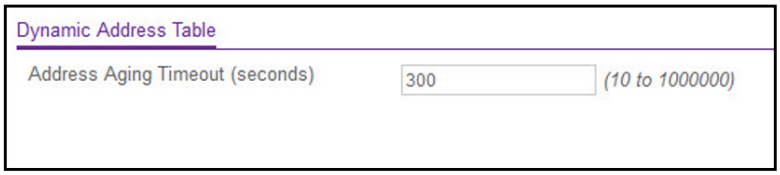
   The login window opens.

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**.



6. In the **Address Aging Timeout (seconds)** field, specify the time-out period in seconds for aging out dynamically learned forwarding information.

   802.1D-1990 recommends a default of 300 seconds. The value can be any number between 10 and 1000000 seconds. The default is 300.

7. Click the **Apply** button.

   Your settings are saved.

Add a Static MAC Address to the MAC Address Table

To add a static MAC address to the MAC Address Table:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

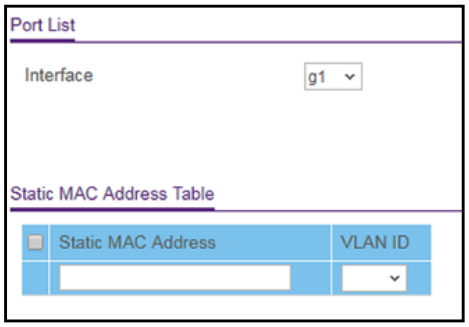
   The login window opens.

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**.



6. From the **Interface** menu, select the interface.
7. In the **Static MAC Address** field, enter the static MAC address that you want to add.
8. From the **VLAN ID** menu, select the VLAN ID that must be associated with the MAC address.
9. Click the **Add** button.

   The static MAC address is added to the switch.

Configure Layer 2 Loop Protection

Loops inside a network are costly because they consume resources and reduce the performance of the network. Detecting loops manually can be cumbersome.

The switch can automatically identify loops in the network. You can enable loop protection per port or globally.

If loop protection is enabled, the switch sends predefined PDU packets to a Layer 2 broadcast destination address (FF:FF:FF:FF:FF:FF) on all ports for which the feature is enabled. You can selectively disable PDU packet transmission for loop protection on specific ports even while port loop protection is enabled. If the switch receives a packet with the previously mentioned broadcast destination address, the source MAC address in the packet is compared with the MAC address of the switch. If the MAC address does not match, the packet is forwarded to all ports that are members of the same VLAN, just like any other broadcast packet. The packet is not forwarded to the port from which it was received.

If the source MAC address matches the MAC address of the switch, the switch can perform one of the following actions, depending on how you configure the action:

- The port is shut down.
- A log message is generated. (If a syslog server is configured, the log message can be sent to the syslog server.)
- The port is shut down and a log message is generated.

Loop protection is not intended for ports that serve as uplinks between spanning tree–aware switches. It is intended for unmanaged switches that drop spanning tree BPDUs. Loop protection detects physical and logical loops between Ethernet ports on a device. You must enable loop protection globally before you can enable and configure it at the interface level. Loop protection is supported on physical interfaces and static LAG interfaces, but not on dynamic LAG interfaces.

Configure Global Layer 2 Loop Protection

To configure L2 loop protection globally:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

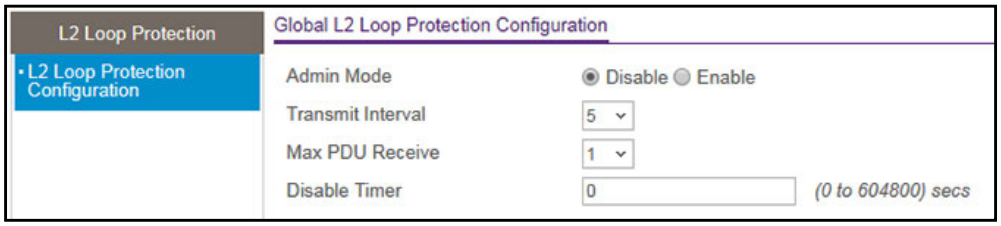
The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > L2 Loop Protection > L2 Loop Protection Configuration**.



6. To enable or disable loop protection feature, select the Admin Mode **Enable** or **Disable** radio button.

   By default, the **Disable** radio button is selected.

7. From the **Transmit Interval** menu, select the time in seconds between transmission of loop packets.

   The default transmit interval is 5 seconds.

8. From the **Max PDU Receive** menu, select the maximum number of packets to be received before an action is taken.

   The default is 1.

9. In the **Disable Timer** field, enter the time in seconds after which a port is disabled when a loop is detected.

   The range is from 0 to 604800 seconds. The default is 0 seconds.

10. Click the **Apply** button.

    Your settings are saved.

View and Configure Layer 2 Loop Protection on a Port

To view and configure L2 loop protection on a port:

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

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

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

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

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

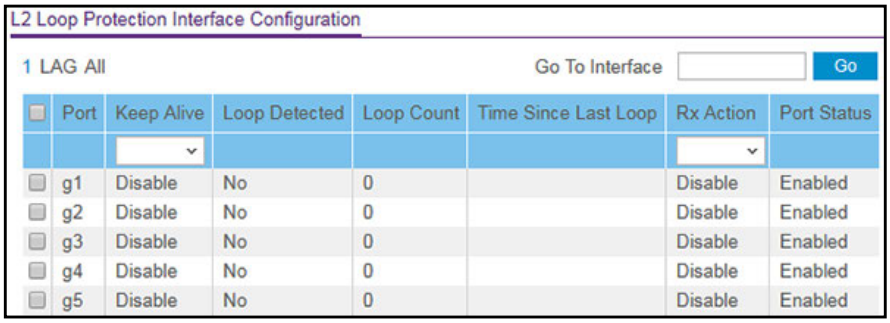
The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > L2 Loop Protection > L2 Loop Protection Configuration**.



6. Use one of the following methods to narrow down the ports that are displayed:
   - To display all the physical ports, click the **1** link.
   - To display all LAGs only, click the **LAG** link.
   - To display all ports and LAGs, click the **All** link.
   - In the **Go To Port** field, type the port number, for example g18, and click the **Go** button.
7. Select one or more check boxes for to the left of the Port column.
8. From the **Keep Alive** menu, select **Enable** or **Disable** to specify whether keep-alives are enabled on an interface.

   The default is Disable.

9. From the **RX Action** menu, select the action that occurs when the switch detects a loop on an interface:
   - **Log**. The switch logs a message.
   - **Disable**. The switch disables the interface. This is the default action.
   - **Both**. The switch both logs a message and disables the interface.
10. Click the **Apply** button.

    Your settings are saved.

11. Click the **Clear** button to clear all the statistics in the table.
12. Click the **Update** button to update the page to show the latest information.

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

Table 40. L2 Loop Protection Interface Information

Field	Description
Loop Detected	Shows whether a loop is detected on the interface. If the interface is disabled and then reenabled, the status changes to No again.
Loop Count	The number of packets that were received after the loop was detected.
Time Since Last Loop	The time that elapsed since the loop was detected.
Port Status	The status of the interface (Enabled, Disabled, or D-Disabled, which stands for diagnostically disabled).

4

Configure Quality of Service

This chapter contains the following sections.

- Quality of Service Concepts
- Manage Class of Service
- Manage Differentiated Services

Quality of Service Concepts

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

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

Manage Class of Service

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

Eight queues per port are supported.

CoS Configuration Concepts

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

Alternatively, when a port is configured as untrusted, it does not trust any incoming packet priority designation and uses the port default priority value instead. All packets arriving at the

ingress of an untrusted port are directed to a specific CoS queue on the appropriate egress ports, in accordance with the configured default priority of the ingress port. This process is also used for cases where a trusted port mapping cannot be honored, such as when a non-IP packet arrives at a port configured to trust the IP DSCP value.

Configure Global CoS Settings

To configure CoS trust mode settings on all interfaces:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

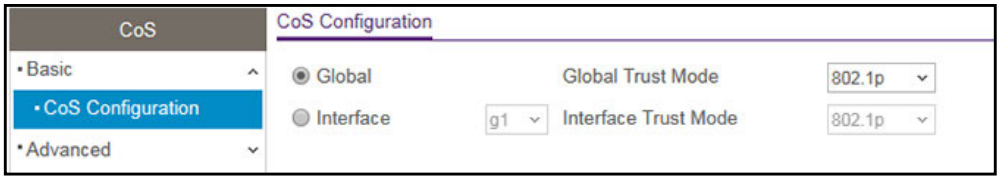
   The login window opens.

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.

   By default, the **Global** radio button is selected.

   - To configure the same CoS trust mode settings for all CoS configurable interfaces, do the following:

     a. Select the **Global** radio button.

     b. From the **Global Trust Mode** menu, select one of the following trust mode options for ingress traffic on the switch:

        - **Untrusted**. Do not trust any CoS packet marking at ingress.
        - **802.1p**. 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 eight 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.

   Your settings are saved.

Configure CoS Interface Settings for an Interface

You can configure the trust mode for one or more interfaces and apply an interface shaping rate to all interfaces or to a specific interface.

To configure CoS settings for an interface:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

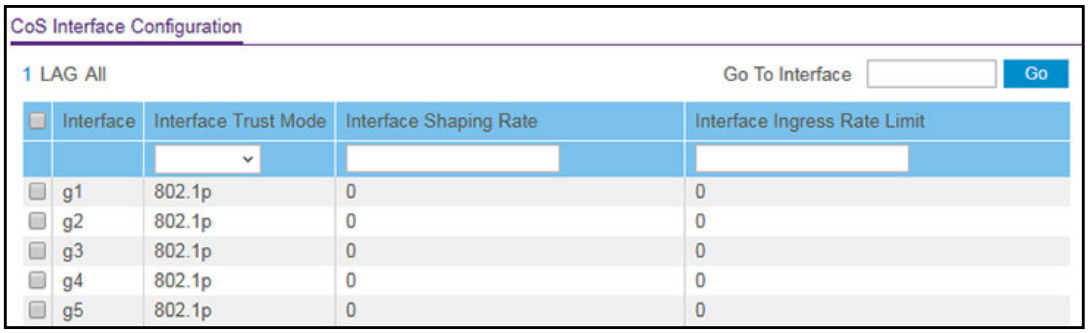
   The login window opens.

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**.



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 value 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 egress bandwidth allowed.

   This setting is used to shape the outbound transmission rate in increments of 1 percent in a range of 0–100. This value is controlled independently of any per-queue maximum bandwidth configuration. It is effectively a second-level shaping mechanism. The default value is 0. The value 0 means that the maximum is unlimited.
10. In the **Interface Ingress Rate Limit** field, specify the maximum ingress bandwidth allowed.

    This setting is used to shape the inbound transmission rate in increments of 1 percent in a range of 0–100. The interface discards traffic that arrives at a bandwidth in excess of the specified limit.
11. Click the **Apply** button.

    Your settings are saved.

Configure CoS Queue Settings for an Interface

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

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

To configure CoS queue settings for an interface:

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

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

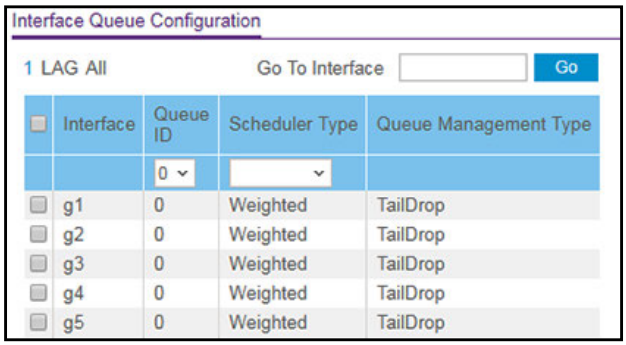
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **QoS > CoS > Advanced > Interface Queue Configuration**.



6. 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.

   You can select a queue from **0** to **7**.

9. From the **Scheduler Type** menu, select one of the following options:
   - **Strict**. The interface services traffic with the highest priority on a queue first.
   - **Weighted**. The interface uses weighted round robin to associate a weight to each queue. This is the default setting.

10. Click the **Apply** button.

    Your settings are saved.

    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.

Map 802.1p Priorities to Queues

You can view or change which internal traffic classes are mapped to the 802.1p priority class values in Ethernet frames that the device receives. The priority-to-traffic class mappings can be applied globally or per interface. The mapping allows the switch to group various traffic types (for example, data or voice) based on their latency requirements and give preference to time-sensitive traffic.

To map 802.1p priorities to queues:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

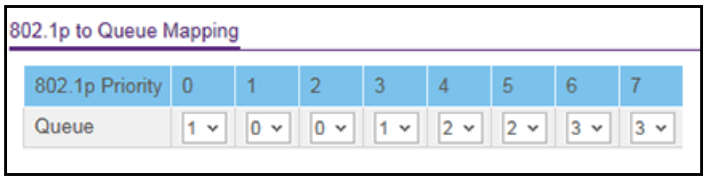
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > CoS > Advanced > 802.1p to Queue Mapping**.



6. In the 802.1p to Queue Mapping table, map each of the eight 802.1p priorities to a queue (internal traffic class) from **0** to **7**.

   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.

   Your settings are saved.

Map DSCP Values to Queues

You can map an internal traffic class to a DSCP value.

To map DSCP values to queues:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

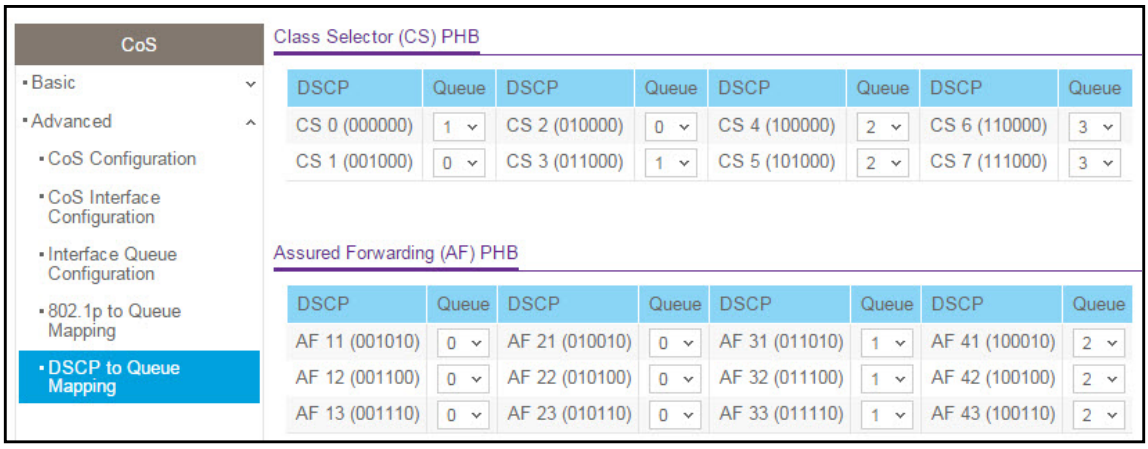
   The login window opens.

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**.



6. For each DSCP value, select from the corresponding **Queue** menu which internal traffic class must be mapped to the DSCP value.

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

   The allowed Per Hop Behavior (PHBs) values, besides other DSCP experimental values, are as follows:

   - **Class Selector (CS) PHB**. These values are based on IP precedence.
   - **Assured Forwarding (AF) PHB**. These values define four main levels to sort and manipulate some flows within the network.
   - **Expedited Forwarding (EF) PHB**. These values are used to prioritize traffic for real-time applications. In many situations, if the network exceeded traffic and you need some bandwidth guaranteed for an application, the EF traffic must receive this rate independently of the intensity of any other traffic attempting to transit the node.

   The Other DSCP Values (Local/Experimental Use) section allows you to set non-default values for advanced settings.

7. Click the **Apply** button.

   Your settings are saved.

Manage Differentiated Services

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

Standard IP-based networks provide best-effort data delivery service. Best-effort service implies that the network delivers the data in a timely fashion, although there is no guarantee. If congestion occurs, packets might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email and file transfers, a slight degradation in service is

acceptable and in many cases unnoticeable. However, any degradation of service can negatively affect applications with strict timing requirements, such as voice and multimedia.

Defining DiffServ

To use DiffServ for QoS, you must first define the following categories and their criteria:

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

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

Note the following about the DiffServ process:

- Packets are filtered and processed based on defined criteria. The filtering criteria is defined by a class. The processing is defined by a policy's attributes. Policy attributes can be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs.
- The configuration process begins with defining one or more match criteria for a class. Then one or more classes are added to a policy. Policies are then added to interfaces.
- Packet processing begins by testing the match criteria for a packet. The *All* class type option specifies that each match criteria within a class must evaluate to true for a packet to match that class. The *Any* class type option specifies that at least one match criteria must evaluate to true for a packet to match that class. Classes are tested in the order in which they were added to the policy. A policy is applied to a packet when a class match within that policy is found.

Configure and Display Global DiffServ Settings

You can display DiffServ general status group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables.

To configure the global DiffServ mode and display DiffServ general status group information:

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

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

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

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

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

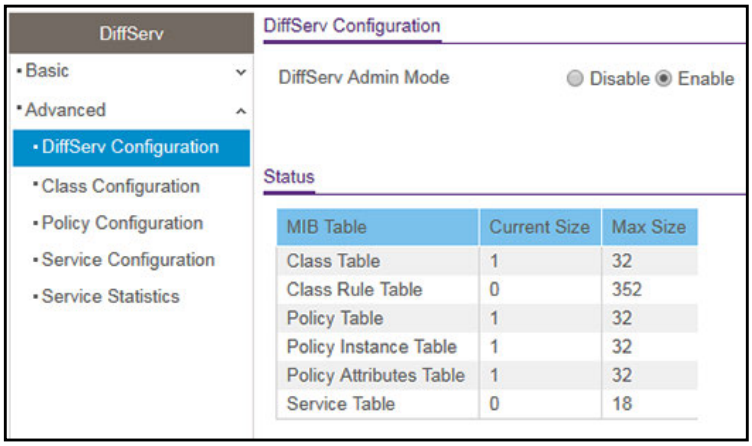
The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > DiffServ > Advanced > DiffServ Configuration**.



6. Select the administrative mode for DiffServ:
   - **Enable**. Differentiated services are active. This is the default setting.
   - **Disable**. The DiffServ configuration is retained and can be changed but is not active.
7. Click the **Apply** button.

   Your settings are saved.

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

Table 41. 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 41. 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.

Add and Configure a DiffServ Class

To add and configure a DiffServ class:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **QoS > DiffServ > Advanced > Class Configuration**.

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

   The Class Name field also lists all existing DiffServ class names, from which you can select one for modification or deletion. The class name can be 1 to 31 alphanumeric characters in length.

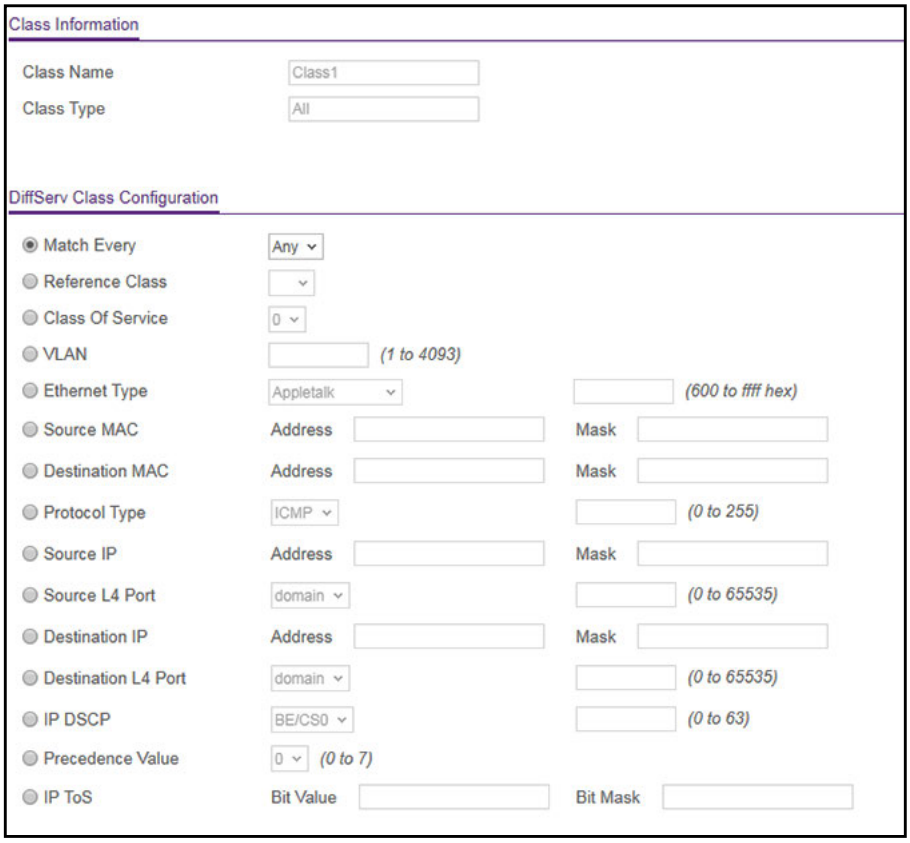
The switch supports only the class type value All, which means that all the various match criteria defined for the class are satisfied for a packet match. All signifies the logical AND statement of all the match criteria. For any class that you add, the class type is All.

7. Click the **Add** button.

   The new class is added.

8. After creating the class, click the class name.

   The class name is a hyperlink to the page on which you can define the class configuration.



9. Define the criteria that must be associated the DiffServ class by selecting *one* of the following radio buttons:

   - **Match Every**. Select this radio button to add a match condition that considers all packets to belong to the class. The only selection from the **Match Every** menu is **Any**.
   - **Reference Class**. Select this radio button to reference another class for criteria. The match criteria defined in the reference class function as match criteria in addition to the match criteria that you define for the selected class. After you select the radio button, the classes that can be referenced are displayed. Select the class to reference. A class can reference only one other class of the same type.
   - **Class of Service**. Select this radio button to require the Class of Service (CoS) value in an Ethernet frame header to match the specified CoS value. This option lists all the

values for the Class of Service match criterion in the range 0 to 7 from which you can select one.

- **VLAN**. Select this radio button to require a packet's VLAN ID to match a VLAN ID. The VLAN value is in the range from 1 to 4093.
- **Ethernet Type**. Select this radio button to require the EtherType value in the Ethernet frame header to match the specified EtherType value. After you select the radio button, select the EtherType keyword from the menu of common protocols that are mapped to their Ethertype value. You can also select **User Value** from the menu and enter a value in the hexadecimal range from 600 to ffff.
- **Source MAC**. Select this radio button to require a packet's source MAC address to match the specified MAC address. After you select this radio button, use the following fields to configure the source MAC address match criteria:
  - **Address**. The source MAC address to match. The source MAC address is specified as six two-digit hexadecimal numbers separated by colons.
  - **Mask**. The MAC mask, which specifies the bits in the source MAC address to compare against the Ethernet frame. Use Fs and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.
- **Destination MAC**. Select this radio button to require a packet's destination MAC address to match the specified MAC address. After you select the radio button, use the following fields to configure the destination MAC address match criteria:
  - **Address**. The destination MAC address to match. The destination MAC address is specified as six two-digit hexadecimal numbers separated by colons.
  - **Mask**. The MAC mask, which specifies the bits in the destination MAC address to compare against an Ethernet frame. Use Fs and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.
- **Protocol Type**. Select this radio button to require a packet's Layer 4 protocol to match the specified protocol, which you must select from the menu. You can also select **Other** from the menu and enter a protocol number from 0 to 255.
- **Source IP**. Select this radio button to require a packet's source IP address to match the specified IP address. After you select the radio button, use the following fields to configure the source IP address match criteria:
  - **Address**. The source IP address format to match in dotted-decimal.
  - **Mask**. The bit mask in IP dotted-decimal format indicating which parts of the source IP address to use for matching against packet content.

- **Source L4 Port**. Select this radio button to require a packet's TCP/UDP source port to match the specified protocol, which you must select from the menu. You can also select **Other** from the menu and enter a port number from 0 to 65535.
- **Destination IP**. Select this radio button to require a packet's destination IP address to match the specified IP address. After you select the radio button, use the following fields to configure the destination IP address match criteria:
  - **Address**. The destination IP address format to match in dotted-decimal.
  - **Mask**. The bit mask in IP dotted-decimal format indicating which parts of the destination IP address to use for matching against packet content.
- **Destination L4 Port**. Select this radio button to require a packet's TCP/UDP destination port to match the specified protocol. You can also select **Other** from the menu and enter a port number from 0 to 65535.
- **IP DSCP**. Select this radio button to require the packet's IP DiffServ Code Point (DSCP) value to match the specified IP DSCP keyword code, which you must select from the menu. You can also select **Other** from the menu and enter an IP DSCP value from 0 to 63. The DSCP value is defined as the high-order 6 bits of the Service Type octet in the IP header.
- **Precedence Value**. Select this radio button to require the packet's IP precedence value to match the specified number from 0 to 7, which you must select from the menu. The IP Precedence field in a packet is defined as the high-order 3 bits of the Service Type octet in the IP header.
- **IP ToS**. Select this radio button to require the packet's Type of Service (ToS) bits in the IP header to match the specified value. The IP ToS field in a packet is defined as all 8 bits of the service type octet in the IP header. After you select the radio button, use the following fields to configure the ToS match criteria:
  - **Bits Value**. Enter a two-digit hexadecimal number octet value in the range from 00 to ff to match the bits in a packet's ToS field.
  - **Bit Mask**. Specify the bit positions that are used for comparison against the IP ToS field in a packet.

10. Click the **Apply** button.

Your settings are saved.

The following table describes the nonconfigurable information displayed in the Class Summary section at the bottom of the DiffServ Class Configuration page.

Table 42. 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 Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **QoS > DiffServ > Advanced > Class Configuration**.

   The Class Name page displays.
6. Select the check box next to the class name.
7. In the **Class Name** field, specify the new name.
8. Click the **Apply** button.

   Your settings are saved.

Change the Criteria for an Existing DiffServ Class

To change the criteria for an existing DiffServ class:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

The default password is **password**.

The System Information page displays.

5. Select **QoS > DiffServ > Advanced > Class Configuration**.

   The Class Name page displays.

6. Click the class name, which is a hyperlink.

   The page on which you can change the class configuration displays.

7. Change the class configuration as needed.
8. Click the **Apply** button.

   Your settings are saved.

Delete a DiffServ Class

To delete a DiffServ class:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > DiffServ > Advanced > Class Configuration**.

   The Class Name page displays.

6. Select the check box next to the class name.
7. Click the **Delete** button.

   The class is removed.

Configure a DiffServ Policy

You can associate a collection of classes with one or more policies.

Create and Configure a DiffServ Policy

To create and configure a DiffServ policy:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

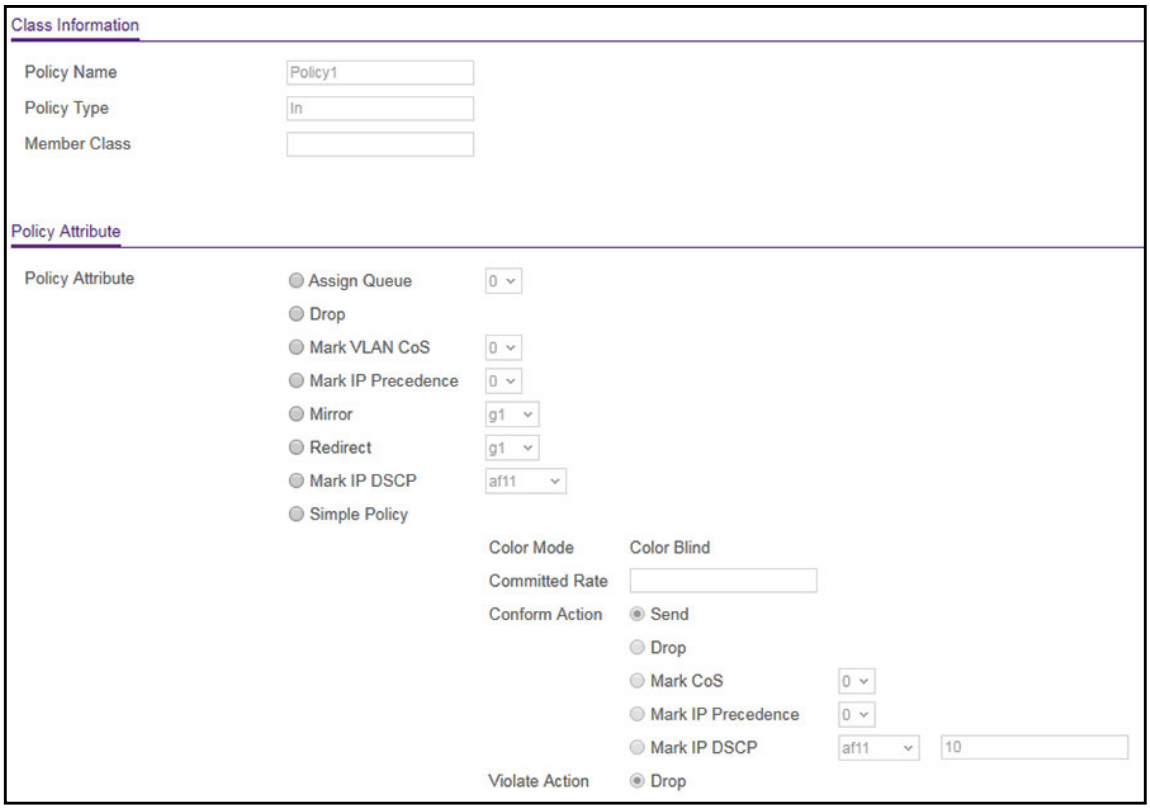
   The System Information page displays.
5. Select **QoS > DiffServ > Advanced > Policy Configuration**.

   The Policy Configuration page displays.
6. Enter a policy name in the **Policy Name** field.

   You cannot specify the policy type. By default, the policy type is In, indicating that the policy applies to ingress packets.
7. From the **Member Class** menu, optionally select an existing class that you want to associate with the new policy.
8. Click the **Add** button.

   The new policy is added.
9. After creating the policy, click the policy name.

   The policy name is a hyperlink to the page on which you can define the policy attributes.



10. Configure the policy attributes by selecting *one* of the following radio buttons:

- **Assign Queue**. Select this radio button to specify that traffic must be assigned to a queue, which you must select from the menu. The queue is expressed as a value in the range from 0 to 7.
- **Drop**. Select this radio button to require each inbound packet to be dropped.
- **Mark VLAN CoS**. Select this radio button to specify the VLAN priority, which you must select from the menu. The VLAN priority is expressed as a value in the range from 0 to 7.
- **Mark IP Precedence**. Select this radio button to require packets to be marked with an IP precedence value before being forwarded. You must select an IP precedence value from 0 to 7 from the menu.
- **Mirror**. Select this radio button to require packets to be mirrored to an interface or LAG, one of which you must select from the menu.
- **Redirect**. Select this radio button to require packets to be redirected to an interface or LAG, one of which you must select from the menu.
- **Mark IP DSCP**. Select this radio button to require packet to be marked with an IP DSCP keyword code, which you must select from the menu. The DSCP value is defined as the high-order 6 bits of the Service Type octet in the IP header.
- **Simple Policy**. Select this radio button to define the traffic policing style for the class. By default, this simple policy is color blind, and color classes do not apply. A simple policy supports a single data rate and results in one of two outcomes: conform or violate. Packets that violate the policy are always dropped. That is, you cannot

specify any other action for those packets. You must specify a policy action for packets that conform to the policy.

- **Committed Rate**. Enter the committed rate that is applied to conforming packets by specifying a value in the range from 1 to 4294967295 Kbps.
- In the Conform Action section, select *one* of the following radio buttons:
  - **Send**. Packets are forwarded unmodified. This is the default confirming action.
  - **Drop**. Packets are dropped. This is the default (and only) violating action.
  - **Mark CoS**. Packets are marked by DiffServ with the specified CoS value before being forwarded. This selection requires that the Mark CoS field is set. You must select a CoS value from 0 to 7 from the menu.
  - **Mark IP Precedence**. These packets are marked by DiffServ with the specified IP Precedence value before being forwarded. This selection requires that the Mark IP Precedence field is set. You must select an IP precedence value from 0 to 7 from the menu.
  - **Mark IP DSCP**. Packets are marked by DiffServ with the specified DSCP value before being forwarded. This selection requires that the DSCP field is set. You must either select a DSCP code from the menu or enter an IP DSCP value from 0 to 63 in the field next to the menu. A value that you enter in the field overrides any selection from the menu.
    The DSCP value is defined as the high-order six bits of the Service Type octet in the IP header.

11. Click the **Apply** button.

Your settings are saved.

Rename an Existing DiffServ Policy

To rename an existing DiffServ policy:

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

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

2. Launch a web browser.

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

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

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

The login window opens.

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

The default password is **password**.

The System Information page displays.

5. Select **QoS > DiffServ > Advanced > Policy Configuration**.

   The Policy Configuration page displays.
6. Select the check box next to the policy name.
7. In the **Policy Name** field, specify the new name.
8. Click the **Apply** button.

   Your settings are saved.

Change the Policy Attributes for an Existing DiffServ Policy

To change the policy attributes for an existing DiffServ policy:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **QoS > DiffServ > Advanced > Policy Configuration**.

   The Policy Configuration page displays.
6. Click the policy name, which is a hyperlink.

   The page on which you can change the policy attributes displays.
7. Change the policy attributes as needed.
8. Click the **Apply** button.

   Your settings are saved.

Remove a Class From an Existing DiffServ Policy

To remove a class from an existing DiffServ policy:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **QoS > DiffServ > Advanced > Policy Configuration**.

   The Policy Configuration page displays.
6. Select the check box next to the policy name.
7. From the **Member Class** menu, select **None**.
8. Click the **Apply** button.

   The class is removed from the policy.

Delete a DiffServ Policy

To delete a DiffServ policy:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **QoS > DiffServ > Advanced > Policy Configuration**.

   The Policy Configuration page displays.

6. Select the check box next to the policy name.
7. Click the **Delete** button.

   The policy is removed.

Configure the DiffServ Service Interface

You can assign (attach) a policy to an interface.

Attach a DiffServ Policy to an Interface

To attach a DiffServ policy to an interface:

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

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

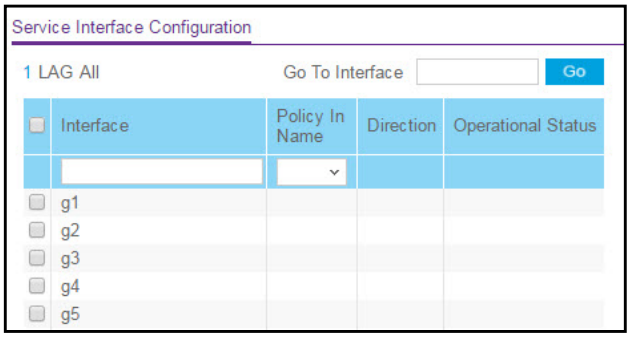
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **QoS > DiffServ > Advanced > Service Configuration**.



6. Select 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.

   Your settings are saved.

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

Table 43. Service Interface Configuration information

Field	Description
Direction	Shows the traffic direction of this service interface, which is always inbound (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 Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **QoS > DiffServ > Advanced > Service Configuration**.

   The Service Interface Configuration page displays.
6. Select the check boxes that are associated with the interfaces from which you want to remove the policy.
7. From the **Policy In Name** menu, select **None**.
8. Click the **Apply** button.

   Your settings are saved.

View DiffServ Service Statistics

You can display service-level statistical information about all interfaces to which DiffServ policies are attached.

To view the DiffServ service statistics:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **QoS > DiffServ > Advanced > Service Statistics**.

   The Service Statistics page displays.
6. Click the **Update** button to refresh the page with the latest information about the switch.

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

Table 44. DiffServ Service Statistics information

Field	Description
Interface	All valid port numbers on the switch with a DiffServ policy that is attached in the inbound direction.
Direction	The traffic direction of interface is inbound (In). This field shows only the direction for which a DiffServ policy is attached.
Policy Name	The name of the policy that is currently attached to the specified interface and direction.
Operational Status	The operational status of the policy that is attached to the specified interface and direction. The value is either Up or Down.
Member Classes	All DiffServ classes that are defined as members of the selected policy name. Select a member class name to display its statistics. If no class is associated with the selected policy, then the list is empty.

5

Manage Device Security

This chapter contains the following sections:

- Configure the Management Security Settings
- Configure Management Access
- Configure Port Authentication
- Set Up Traffic Control
- Configure Access Control Lists

Configure the Management Security Settings

You can configure the login password, Remote Authorization Dial-In User Service (RADIUS) settings, Terminal Access Controller Access Control System (TACACS) settings, and authentication lists.

Change the Password for the Local Browser Interface

You can change the login password for the default user with the user name admin.

To change the login password for the local browser interface:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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**.

   The Change Password page displays.
6. In the **Current Password** field, enter the current password.

   The default password is **password**. The password is displayed in dots.
7. In the **New Password** field, specify the new password.

   The password is displayed in dots. A password can be up to 20 alphanumeric characters in length, and is case-sensitive.
8. In the **Confirm Password** field, enter the password again to confirm that you entered it correctly.

   The password is displayed in dots.

9. Click the **Apply** button.

   Your settings are saved.

Note: If you forget the password and are unable to log in to the switch local browser interface, press the **Factory Defaults** button on the front panel of the switch for more than five seconds. The device reboots, and all switch settings, including the password, are reset to the factory default values.

Manage the RADIUS Settings

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

- Web access
- Access control port (802.1X)

Configure the Global RADIUS Server Settings

You can add information about one or more RADIUS servers on the network.

If you configure multiple RADIUS servers, consider the maximum delay time when you specify the maximum number of retransmissions (that is, the value that you enter in the **Max Number of Retransmits** field) and the time-out period (that is, the value that you enter in the **Timeout Duration** field) for RADIUS:

For one RADIUS server, a retransmission does not occur until the configured time-out period expires without a response from the RADIUS server. In addition. the maximum number of retransmissions for one RADIUS server must pass before the switch attempts the next RADIUS server.

Therefore, the maximum delay in receiving a RADIUS response on the switch equals the maximum number of retransmissions multiplied by the time-out period multiplied by the number of configured RADIUS servers. If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the switch receives a RADIUS response.

To configure the global RADIUS server settings:

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

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

2. Launch a web browser.

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

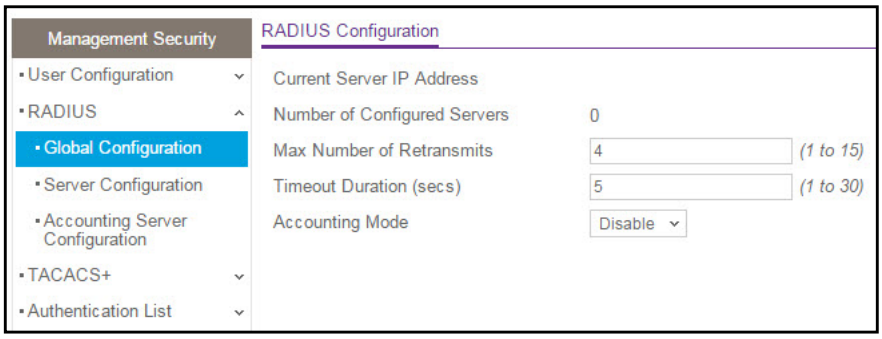
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > RADIUS > Global Configuration**.



   The Current Server IP Address field is blank if no servers are configured (see Configure a RADIUS Authentication Server on the Switch on page 202). 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.

CAUTION:

The maximum delay in receiving a RADIUS response on the switch equals the maximum number of retransmissions multiplied by the time-out period multiplied by the number of configured RADIUS servers. If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the switch receives a RADIUS response.

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

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

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

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

8. From he **Accounting Mode** menu, select to disable or enable RADIUS accounting on the server.

   The default is Disabled.

9. Click the **Apply** button.

   Your settings are saved.

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

Table 45. RADIUS Configuration information

Field	Description
Current Server IP Address	The IP address of the current server. This field is blank if no servers are configured.
Number of Configured Servers	The number of configured authentication RADIUS servers. The value can range from 0 to 3.

Configure a RADIUS Authentication Server on the Switch

You view and configure various settings for a RADIUS server configured on the switch.

Add a Primary RADIUS Authentication Server to the Switch

To add a primary RADIUS authentication server to the switch and view or reset the RADIUS authentication server statistics:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

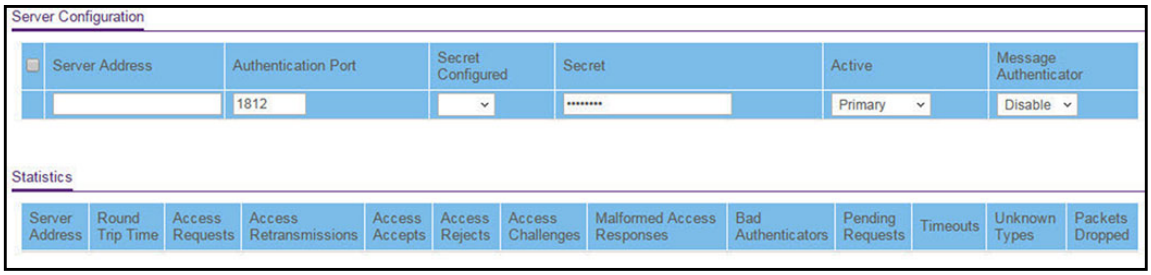
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > RADIUS > Server Configuration**.



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

   The range is from 1 to 65535. The default value is 1812.
8. From the **Secret Configured** menu, select **Yes**.

   You must select **Yes** before you can configure the RADIUS secret. After you add the RADIUS server, this field indicates whether the shared secret for this server was configured.
9. In the **Secret** field, type the shared secret text string used for authenticating and encrypting all RADIUS communications between the switch and the RADIUS server.

   This secret must match the RADIUS encryption.
10. From the **Active** menu, select **Primary**.
11. From the **Message Authenticator** menu, select **Enable** or **Disable** to specify whether the message authenticator attribute for the selected server is enabled.

    The message authenticator adds protection to RADIUS messages by using an MD5 hash to encrypt each message. The shared secret is used as the key, and if the message fails to be verified by the RADIUS server, it is discarded.
12. Click the **Add** button.

    The server is added to the switch.
13. To reset the authentication server and RADIUS statistics to their default values, click the **Clear Counters** button.

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

Table 46. RADIUS authentication server statistics information

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.
Access Requests	The number of RADIUS access-request packets sent to this server. This number does not include retransmissions.

Table 46. RADIUS authentication server statistics information (continued)

Field	Description
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.

Modify the Settings for a RADIUS Authentication Server on the Switch

To modify the settings for a RADIUS authentication server on the switch:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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.

   Your settings are saved.

Remove a RADIUS Authentication Server From the Switch

To remove a RADIUS authentication server from the switch:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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.

   Your settings are saved.

Configure a RADIUS Accounting Server

You can view and configure various settings for a RADIUS accounting server on the network.

Add a RADIUS Accounting Server to the Switch

To add a RADIUS accounting server to the switch and view or clear the RADIUS accounting server statistics:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

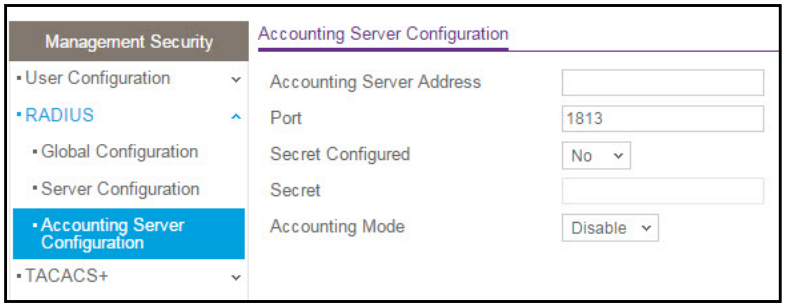
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > RADIUS > Accounting Server Configuration**.



6. In the **Accounting Server Address** field, specify the IP address of the RADIUS accounting server to add.
7. In the **Port** field, specify the UDP port number that the server uses to verify the RADIUS accounting server authentication. The default UDP port number is 1813.
8. From the **Secret Configured** menu, select **Yes** to add a RADIUS secret in the next field.

   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 **Apply** button.

    Your settings are saved.

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

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

Table 47. RADIUS accounting server statistics information

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.

Modify the Settings for the RADIUS Accounting Server on the Switch

To modify the settings for the RADIUS accounting server on the switch:

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

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

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

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

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

The login 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. Modify the configuration for the accounting server.
7. Click the **Apply** button.

   Your settings are saved.

Remove the RADIUS Accounting Server From the Switch

To remove the RADIUS accounting server from the switch:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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. Remove the server IP address from the **Accounting Server Address** field.

   Leave the field blank.

7. Click the **Apply** button.

   Your settings are saved. The RADIUS accounting server is removed.

Configure TACACS+

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

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

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

Configure the Global TACACS+ Settings

You can configure the global TACACS+ settings for communication between the switch and a TACACS+ server.

To configure the global TACACS+ settings:

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

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

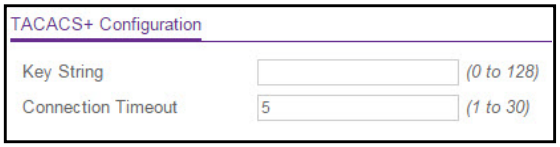
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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**.



6. In the **Key String** field, specify the authentication and encryption key for TACACS+ communications between the switch and the TACACS+ server.

   The range is from 0 to 128. The key must match the key configured on the TACACS+ server.

7. In the **Connection Timeout** field, specify the maximum number of seconds allowed to establish a TCP connection between the switch and the TACACS+ server.\

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

8. Click the **Apply** button.

   Your settings are saved.

Configure a TACACS+ Server on the Switch

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

To configure a TACACS+ server on the switch:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

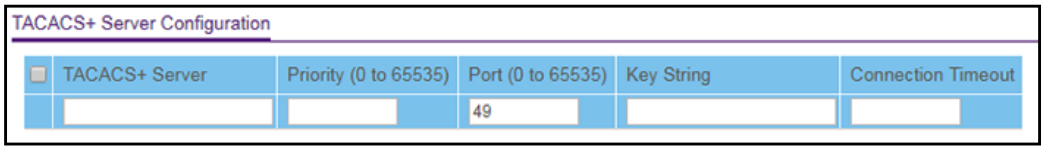
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security> TACACS+ > TACACS+ Server Configuration**.



6. In the **TACACS+ Server** field, enter the TACACS+ server IP address.
7. In the **Priority** field, specify the priority for the TACACS+ server.

   The priority determines the order in which the TACACS+ servers are contacted when attempting to authenticate a user. A value of 0 is the highest priority. The range is from 0 to 65535.

8. In the **Port** field, specify the authentication port value for TACAS+ server sessions.

   The value must be in the range from 0 to 65535. If you do not specify a value, the switch uses the standard TCP port 49 for sessions with the server.

9. In the **Key String** field, specify the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server.

   The range is from 0 to 128. The key must match the key used on the TACACS+ server.

10. In the **Connection Timeout** field, specify the time that passes before the connection between the device and the TACACS+ server times out.

    The range is from 1 to 30. If you do not specify a value, the switch uses a default value of 5 seconds.

11. Click the **Add** button.

    The server is added to the switch.

Modify the Settings for a TACACS+ Server on the Switch

To modify the settings for a TACACS+ server on the switch:

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

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security> TACACS+ > TACACS+ Server Configuration**.

   The TACACS+ Server Configuration page displays.

6. Select the check box next to the server IP address.
7. Modify the configuration for the selected TACACS+ server.
8. Click the **Apply** button.

   Your settings are saved.

Remove a TACACS+ Server From the Switch

To remove a TACACS+ server from the switch:

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

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

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

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Security > Management Security> TACACS+ > TACACS+ Server Configuration**.

   The TACACS+ Server Configuration page displays.
6. Select the check box next to the server IP address.
7. Click the **Delete** button.

   The TACACS+ server is removed.

Configure Authentication Lists

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

Note: The admin user is assigned to a preconfigured list that is named defaultList and that you cannot delete.

Configure an HTTP Authentication List

You can configure the default HTTP login list.

To change the HTTP authentication method for the default list:

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

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

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

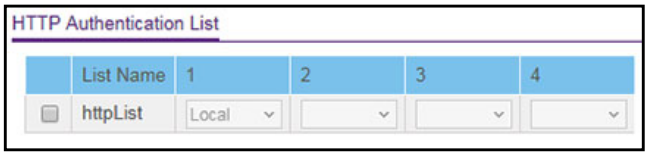
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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**.



6. Select the check box next to the httpList name.
7. From the menu in the 1 column, select the authentication method that must be used first in the selected authentication login list.

   If you select a method that does not time out as the first method, such as **Local**, no other method is tried, even if you specified more than one method. User authentication occurs in the order the methods are selected. Possible methods are as follows:

   - **Local**. The user's locally stored ID and password are used for authentication. Since the Local method does not time out, if you select this option as the first method, no other method is tried, even if you specified more than one method. This is the default method. This is the default selection for Method 1.
   - **RADIUS**. The user's ID and password are authenticated using the RADIUS server. If you select **RADIUS** or **TACACS+** as the first method and an error occurs during the authentication, the switch uses Method 2 to authenticate the user.
   - **TACACS+**. The user's ID and password are authenticated using the TACACS+ server. If you select **RADIUS** or **TACACS+** as the first method and an error occurs during the authentication, the switch attempts user authentication Method 2.
   - **None**. The authentication method is unspecified, that is, no authentication is required.
8. From the menu in the 2 column, select the authentication method, if any, that must be used second in the selected authentication login list.

   This is the method that is used if the first method times out. If you select a method that does not time out as the second method, the third method is not tried.
9. From the menu in the 3 column, select the authentication method, if any, that must be used third in the selected authentication login list.

10. From the menu in the 4 column, select the method, if any, that must be used fourth in the selected authentication login list.

    This is the method that is used if all previous methods time out.

11. Click the **Apply** button.

    Your settings are saved.

Configure an HTTPS Authentication List

You can configure the default login list for secure HTTP (HTTPS).

To configure an HTTPS authentication list:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

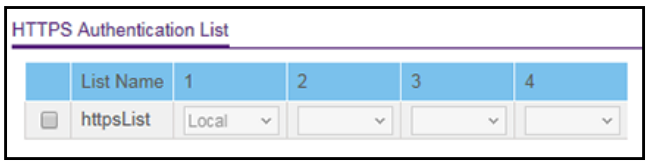
   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > Authentication List > HTTPS Authentication List**.



6. Select the check box next to the httpsList name.
7. From the menu in the 1 column, select the authentication method that must be used first in the selected authentication login list.

   If you select a method that does not time out as the first method, such as **Local**, no other method is tried, even if you specified more than one method. This setting does not display when you first create a new login list. User authentication occurs in the order the methods are selected. Possible methods are as follows:

   - **Local**. The user's locally stored ID and password are used for authentication. Since the Local method does not time out, if you select this option as the first method, no

other method is tried, even if you specified more than one method. This is the default selection for Method 1.

- **RADIUS**. The user's ID and password are authenticated using the RADIUS server. If you select **RADIUS** or **TACACS+** as the first method and an error occurs during the authentication, the switch uses Method 2 to authenticate the user.
- **TACACS+**. The user's ID and password are authenticated using the TACACS+ server. If you select **RADIUS** or **TACACS+** as the first method and an error occurs during the authentication, the switch attempts user authentication Method 2.
- **None**. The authentication method is unspecified, that is, no authentication is required.

8. From the menu in the 2 column, select the authentication method, if any, that must be used second in the selected authentication login list.

   This is the method that is used if the first method times out. If you select a method that does not time out as the second method, the third method is not tried.

9. From the menu in the 3 column, select the authentication method, if any, that must be used third in the selected authentication login list.
10. From the menu in the 4 column, select the method, if any, that must be used fourth in the selected authentication login list.

    This is the method that is used if all previous methods time out.

11. Click the **Apply** button.

    Your settings are saved.

Configure the Dot1x Authentication List

The Dot1x authentication list defines the IEEE 802.1X authentication method used for the default list. The default list is dot1xList.

To configure the dot1x authentication list:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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 > Dot1x Authentication List**.

   The Dot1x Authentication List page displays.

6. Select the check box next to dot1xList.
7. From the menu in the 1 column, select the method that must be used first in the selected authentication login list.

   The options are as follows:

   - **Radius**. The user's ID and password are authenticated using the RADIUS server instead of locally.
   - **None**. The user is not authenticated.

8. Click the **Apply** button.

   Your settings are saved.

Manage the Smart Control Center Utility

You can enable or disable the SCC administrative mode.

To enable or disable the SCC administrative mode:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > SCC Control**.

   The NETGEAR Smart Control Center (SCC) Utility page displays.

6. Select the one of the following SCC Admin Mode radio buttons:
   - **Enable**. SCC can discover the switch and perform actions on the switch. This is the default setting.
   - **Disable**. SCC can discover the switch but cannot perform any actions on the switch.

Note: Because the switch administrator password is contained in each NETGEAR Switch Discovery Protocol (NSDP) packet, disabling SCC increases the switch security.

7. Click the **Apply** button.

   Your settings are saved.

Configure Management Access

You can configure HTTP and secure HTTP access to the switch local browser interface. You can also configure access control profiles and access rules.

Configure HTTP Access Settings

You can configure the HTTP access settings on the switch.

To configure the HTTP access settings:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

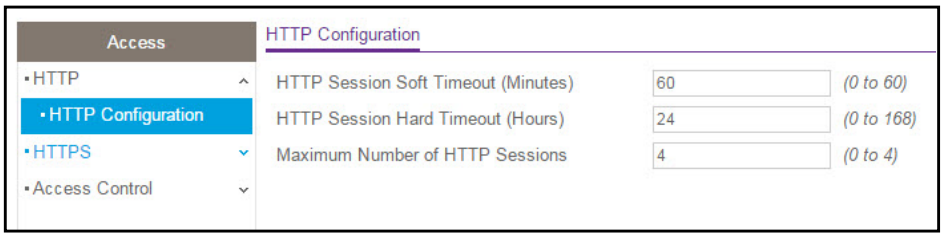
   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Access > HTTP > HTTP Configuration**.



6. In the **HTTP Session Soft Timeout** field, specify the number of minutes an HTTP session can be idle before a time-out occurs.

   The value must be in the range from 0 to 60 minutes. The default value is 5 minutes.

   After the session is inactive for the configured time, you are automatically logged out and must reenter the password to access the local browser interface A value of zero means that the session does not time out.

7. In the **HTTP Session Hard Timeout** field, specify the hard time-out for HTTP sessions.

   This time-out is unaffected by the activity level of the session. The value must be in the range from 0 to 168 hours. A value of zero means that the session does not time out. The default value is 24 hours.

8. In the **Maximum Number of HTTP Sessions** field, specify the maximum number of HTTP sessions that can exist at the same time.

   The range is from 1 to 4 sessions. The default is 4 sessions.

9. Click the **Apply** button.

   Your settings are saved.

Configure HTTPS Access Settings

Secure HTTP enables the transmission of HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. When you manage the switch by using a web interface, Secure HTTP can help ensure that communication between the management system and the switch is protected from eavesdroppers and man-in-the-middle attacks. The hash algorithms that SSL uses are MD5 and SHA-1.

To configure HTTPS access settings:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

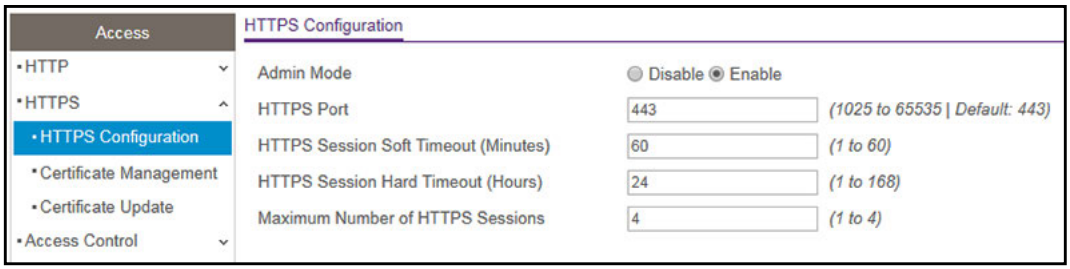
   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Access > HTTPS > HTTPS Configuration**.



6. Select the Admin Mode **Enable** or **Disable** radio button.

   This selection enables or disables secure HTTP (HTTPS). The default value is Enable. You can download SSL certificates only when HTTPS is disabled. You can enable HTTPS only if a certificate is present on the device.

7. In the **HTTPS Port** field, type the HTTPS port number.

   The range is from 1025 to 65535. The default is port 443.

8. In the **HTTPS Session Soft Timeout (Minutes)** field, enter the inactivity time-out for HTTPS sessions.

   The range is from 1 to 60 minutes. The default value is 5 minutes.

9. In the **HTTPS Session Hard Timeout (Hours)** field, set the hard time-out for HTTPS sessions.

   This time-out is unaffected by the activity level of the session. The range is from 1 to 168 hours. The default is 24 hours.

10. In the **Maximum Number of HTTPS Sessions** field, enter the maximum allowable number of HTTPS sessions.

    The range is from 1 to 4 sessions. The default is 4 sessions.

11. Click the **Apply** button.

    Your settings are saved.

Manage Certificates for HTTPS Access

You can manage certificates for HTTPS access.

Generate an SSL Certificate

Note: Before you can generate a certificate, you must disable HTTPS (see Configure HTTPS Access Settings on page 218) and log back in to the local browser interface over an HTTP session. After you generate the certificate, you can reenable HTTPS and log back in to the local browser interface over an HTTPS session.

To generate an SSL certificate:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Access > HTTPS > Certificate Management**.

   The Certificate Present field displays whether a certificate is present on the switch.

6. In the Certificate Management section, select the **Generate Certificates** radio button.
7. Click the **Apply** button.

   The switch generates an SSL certificate.

   The Certificate Generation Status field shows progress information.

Delete an SSL Certificate

Note: Before you can delete a certificate, you must disable HTTPS (see Configure HTTPS Access Settings on page 218) and log back in to the local browser interface over an HTTP session. After you generate the certificate, you can reenable HTTPS and log back in to the local browser interface over an HTTPS session.

To delete an SSL certificate:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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 section, select **Delete Certificates** radio button.
8. Click the **Apply** button.

   The certificate is removed.

Transfer an Existing Certificate to the Switch

You can transfer a certificate file to the switch.

For the switch to accept HTTPS connections from a device, the switch requires a public key certificate. You can generate a certificate externally (for example, offline) and transfer it to the switch.

Before you transfer a file from a TFTP server to the switch, the following conditions must be true:

- The file that you transfer from a TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch contains a path to the TFTP server.

Note: Before you can transfer a certificate, you must disable HTTPS (see Configure HTTPS Access Settings on page 218) and log back in to the local browser interface over an HTTP session. After you generate the certificate, you can reenable HTTPS and log back in to the local browser interface over an HTTPS session.

To configure the certificate transfer settings for HTTPS sessions:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

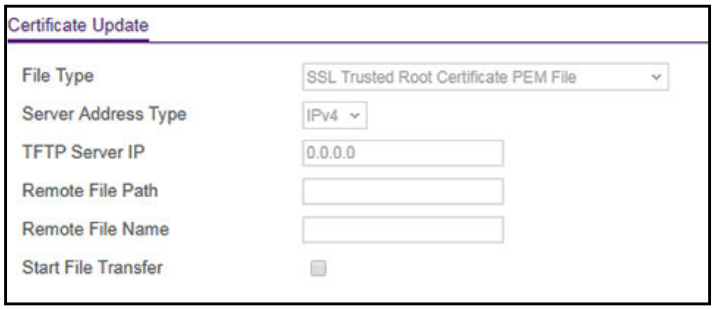
   The login window opens.

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 Update**.



6. From the **File Type** menu, select the type of SSL certificate to download, which can be one of the following:
   - **SSL Trusted Root Certificate PEM File**. SSL Trusted Root Certificate file (PEM Encoded)
   - **SSL Server Certificate PEM File**. SSL Server Certificate File (PEM Encoded)
   - **SSL DH Weak Encryption Parameter PEM File**. SSL Diffie-Hellman Weak Encryption Parameter file (PEM Encoded)
   - **SSL DH Strong Encryption Parameter PEM File**. SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded)
7. From the **Server Address Type** menu, select **IPv4** or **DNS** to indicate the format for the TFTP Server IP field.

   The default is IPv4.
8. In the **TFTP Server IP** field, specify the address or host name of the TFTP server.

   The address can be an IP address in standard x.x.x.x format or a host name. The host name must start with a letter of the alphabet.
9. In the **Remote File Path** field, enter the path of the file to download.

   You can enter up to 96 characters. The default is blank.
10. In the **Remote File Name** field, enter the name of the file on the TFTP server to download.

    You can enter up to 32 characters. The default is blank.
11. Select the **Start File Transfer** check box.
12. Click the **Apply** button.

    The file transfer starts. A status message displays during the transfer and upon successful completion of the transfer.

Manage Access Control to the Switch

Access control allows you to configure an access control profile and set rules for access to the local browser interface, access by SNMP stations, and client access to a TFTP server. We refer to an access control profile as an access profile. You can add a single access profile, which you can configure, activate, or deactivate.

CAUTION:

If you configure a security access profile incorrectly and you activate the access profile, you might no longer be able to access the switch's local browser interface. If that situation occurs, you must reset the switch to factory default settings (see Reset the Switch to Its Factory Default Settings on page 315).

Add an Access Profile

You can set up a single security access profile with which you can associate an access rule configuration.

To add an access profile:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

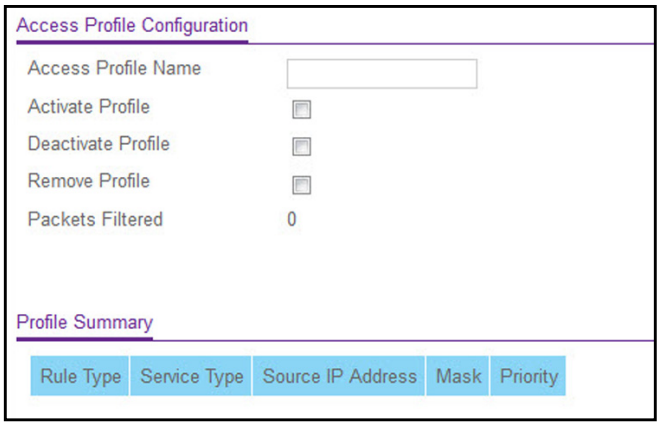
   The login window opens.

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**.



6. In the **Access Profile Name** field, enter the name of the access profile to be added.

   The maximum length is 32 characters.

7. Click the **Apply** button.

   Your settings are saved. By default, the access profile is deactivated. After you add rules, you can activate the access profile.

Add a Rule to the Access Profile

After you add the access profile, you can add one or more security access rules to the access profile.

If you access the switch from a computer over an HTTPS sessions, make sure that you do add a permit rule for an HTTPS session with your computer's IP address and subnet mask.

CAUTION:

You must add a permit rule for your device and access method, otherwise you are locked out from the switch after you activate the access profile. If that situation occurs, you must reset the switch to factory default settings (see Reset the Switch to Its Factory Default Settings on page 315).

To add a rule to the access profile:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

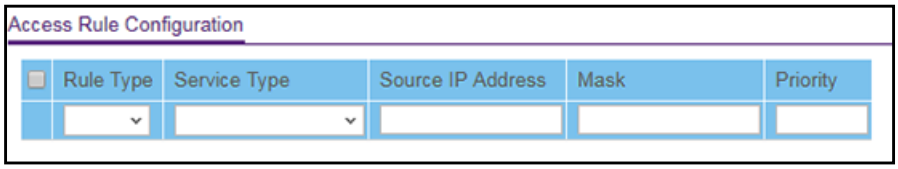
The login window opens.

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**.



6. From the **Rule Type** menu, select **Permit** or **Deny** to permit or deny access when the selected rules are matched.

   A Permit rule allows access from a device that matches the rule criteria. A Deny rule blocks a device that matches the rule criteria.

7. From the **Service Type** menu, select the access method to which the rule is applied.

   The policy is restricted by the selected access method. Possible access methods are **TFTP**, **HTTP, Secure HTTP (SSL)**, and **SNMP**.

8. In the **Source IP Address** field, enter the source IP address from which the management traffic originates.
9. In the **Mask** field, specify the subnet mask from which the management traffic originates.
10. In the **Priority** field, assign a priority to the rule.

    The rules are validated against the incoming management request in ascending order of their priorities. If a rule matches, the action is performed and subsequent rules below that rule are ignored. For example, if a source IP address 10.10.10.10 is configured with priority 1 to permit, and the same source IP address 10.10.10.10 is also configured with priority 2 to deny, then access is permitted if the profile is active, and the second rule is ignored.

11. Click the **Add** button.

    The access rule is added.

Activate the Access Profile

After you add rules to the access profile, you can activate the access profile.

CAUTION:

If you configure a security access profile incorrectly and you activate the access profile, you might no longer be able to access the switch's local browser interface. If that situation occurs, you must reset the switch to factory default settings (see Reset the Switch to Its Factory Default Settings on page 315).

To activate the access profile:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Security > Access > Access Control > Access Profile Configuration**.

   The Access Profile Configuration page displays. The **Deactivate Profile** check box is selected.
6. Select the **Activate Profile** check box.
7. Click the **Apply** button.

   Your settings are saved and the access profile is now active.

Display the Access Profile Summary and the Number of Filtered Packets

After you added rules to the active profile, you can view the entries in the summary. If the access profile is active, you can also view the number of filtered packets.

To display the access profile summary and the number of filtered packets:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

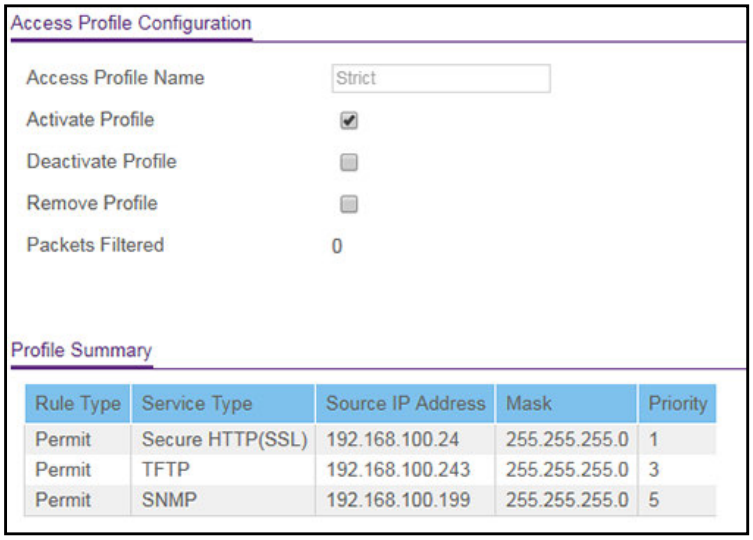
   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Access > Access Control > Access Profile Configuration**.



   The Packets Filtered field displays the number of packets filtered (none in the previous figure).

6. To refresh the page with the latest information about the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

Table 48. Access profile configuration profile summary

Field	Description
Rule Type	The action performed when the rules match.
Service Type	The service type selected. The policy is restricted by the selected service type.
Source IP Address	The source IP address of the client originating the management traffic.
Mask	The subnet mask of the IP Address.
Priority	The priority of the rule.

Deactivate an Access Profile

You can deactivate an access profile.

To deactivate an access profile:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Security > Access > Access Control > Access Profile Configuration**.

   The Access Profile Configuration page displays. The **Activate Profile** check box is selected.
6. Select the **Deactivate Profile** check box.
7. Click the **Apply** button.

   Your settings are saved and the access profile is now deactivated.

Remove an Access Profile

You can remove an access profile that you no longer need. Before you can remove the access profile, you must deactivate it (see Deactivate an Access Profile on page 228).

To remove an access profile:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Security > Access > Access Control > Access Profile Configuration**.

The Access Profile Configuration page displays. The **Deactivate Profile** check box is selected.

6. Select the **Remove Profile** check box.
7. Click the **Apply** button.

   The access profile is removed.

Configure Port Authentication

With port-based authentication, when 802.1X is enabled globally and on the port, successful authentication of any one supplicant attached to the port results in all users being able to use the port without restrictions. At any time, only one supplicant is allowed to attempt authentication on a port in this mode. Ports in this mode are under bidirectional control. This is the default authentication mode.

An 802.1X network includes three components:

- **Authenticator**. The port that is authenticated before access to system services is permitted.
- **Supplicant**. The host that is connected to the authenticated port requesting access to the system services.
- **Authentication Server**. The external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the supplicant is authorized to access system services.

Configure Global 802.1X Settings

You can configure global port access control settings on the switch.

To globally enable the 802.1X features:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

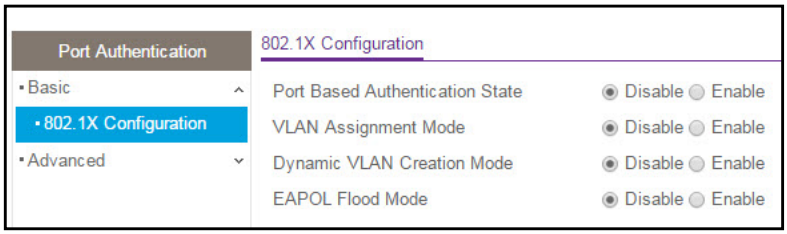
   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

The default password is **password**.

The System Information page displays.

5. Select **Security > Port Authentication > Basic > 802.1X Configuration**.



6. Configure the following port authentication settings:
   - **Port Based Authentication State**. This selection specifies the 802.1X administrative mode on the switch. The default value is Disable.
     - **Enabled**. If 802.1X is enabled, authentication is performed by a RADIUS server. This means that the primary authentication method must be RADIUS. To set the method, select **Security > Management Security > Authentication List** and select **RADIUS** as method 1 for defaultList. For more information, see Configure Authentication Lists on page 212.
     - **Disabled**. When port-based authentication is globally disabled, the switch does not check for 802.1X authentication before allowing traffic on any ports, even if the ports are configured to allow only authenticated users.
   - **VLAN Assignment Mode**. This selection specifies whether a port can be placed in a particular VLAN. The default value is Disable.

     When enabled, this feature allows a port to be placed into a particular VLAN based on the result of the authentication or type of 802.1X authentication a client uses when it accesses the device. The authentication server can provide information to the device about which VLAN to assign the supplicant.
   - **Dynamic VLAN Creation Mode**. This selection specifies whether a VLAN can be dynamically created. The default value is Disable.

     If RADIUS-assigned VLANs are enabled, the RADIUS server includes the VLAN ID in the 802.1X tunnel attributes of its response message to the device. If dynamic VLAN creation is enabled on the device and the RADIUS-assigned VLAN does not exist, the assigned VLAN is dynamically created. This means that the client can connect from any port and is assigned to the appropriate VLAN. This feature gives flexibility for clients to move around the network without much additional configuration required.
   - **EAPOL Flood Mode**. This selection specifies whether Extensible Authentication Protocol (EAP) over LAN (EAPoL) flood support is enabled on the switch. The default value is Disable.
7. Click the **Apply** button.

   Your settings are saved.

Manage Port Authentication on Individual Ports

You can enable and configure port access control on one or more physical ports.

Configure 802.1X Settings for a Port

To configure 802.1X settings for a port:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

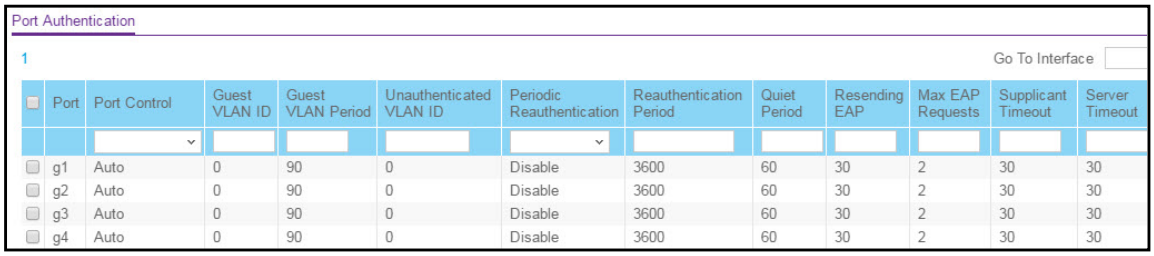
   The login window opens.

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 previous figure shows only part of the page.

6. Use the horizontal scroll bar at the bottom of the page to view all the fields.
7. 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.

8. Specify the following settings:
   - **Port Control**. Defines the port authorization state. The control mode is set only if the link status of the port is link up. Select one of the following options:
     - **Auto**. The switch automatically detects the mode of the interface.

  - **Authorized**. The switch places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication.
  - **Unauthorized**. The switch denies the selected interface system access by moving the interface into unauthorized state. The switch cannot provide authentication services to the client through the interface.
  - **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 range is from 0 to 4093. The default value is 0. Enter 0 to reset the guest VLAN ID on the interface. The guest VLAN allows the port to provide a distinguished service to unauthenticated users, after three authentication failures. This feature provides a mechanism to allow users access to hosts on the guest VLAN.
- **Guest VLAN Period**. Specify the time in 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 from 1 to 300. The default value is 90.
- **Unauthenticated VLAN ID**. Specify the VLAN ID of the unauthenticated VLAN for the selected port. The range is from 0 to 3965. The default value is 0. Hosts that fail the authentication might be denied access to the network or placed on a VLAN created for unauthenticated clients. This VLAN might be configured with limited network access.
- **Periodic Reauthentication**. 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 from 1 to 65535. The default value is 3600. If this field is disabled, connected clients are not forced to reauthenticate periodically.
- **Quiet Period**. Specify the time in seconds that the port remains in the quiet state following a failed authentication exchange. While in the quite state, the port does not attempt to acquire a supplicant.
- **Resending EAP**. Specify the EAP retransmit period for the selected port. The transmit period is the time in seconds, after which an EAPoL EAP Request/Identify frame is resent to the supplicant.
- **MAX EAP Requests**. Specify the maximum number of EAP requests for the 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 time in seconds after which the supplicant times out.
- **Server Timeout**. Specify the time that elapses before the switch resends a request to the authentication server.

9. Click the **Apply** button.

Your settings are saved.

The following table describes the port authentication status information available on the page.

Table 49. 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. The option is Authenticator or Supplicant.
Authenticator PAE State	The current state of the authenticator PAE state machine. The options are as follows: • Initialize • Disconnected • Connecting • Authenticating • Authenticated • Aborting • Held • ForceAuthorized • ForceUnauthorized
Backend State	The current state of the backend authentication state machine. The options 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 Discover or Change the Switch IP Address on page 12.

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

The login 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 Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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 Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

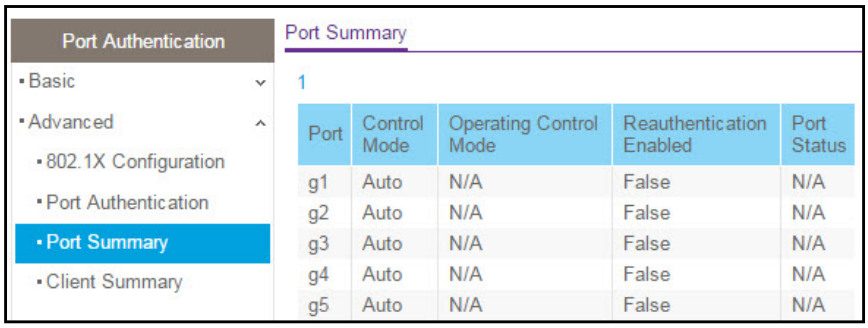
   The login window opens.

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**.



The following table describes the fields on the Port Summary page.

Table 50. Port summary

Field	Description
Port	The port whose settings are displayed in the current table row.
Control Mode	This field indicates the configured control mode for the port. The options are as follows: • **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	The control mode under which the port is actually operating. The options are as follows: • 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 option is True or False. If the value is True, reauthentication occurs. Otherwise, reauthentication is not allowed.
Port Status	The authorization status of the specified port. The options are Authorized, Unauthorized, and N/A. If the port is in detached state, the value is N/A because the port cannot participate in port access control.

View the Client Summary

You can display information about supplicant devices that are connected to the local authenticator ports. If no active 802.1X sessions exist, the table is empty.

To view the client summary:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

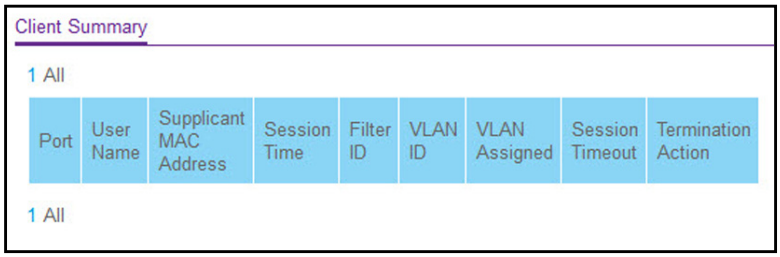
The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Port Authentication > Advanced > Client Summary**.



The following table describes the fields on the Client Summary page.

Table 51. Client Summary information

Field	Description
Port	The port to be displayed.
User Name	The user name representing the identity of the supplicant device.
Supplicant Mac Address	The supplicant's device MAC address.
Session Time	The time since the supplicant logged in seconds.
Filter ID	The policy filter ID assigned by the authenticator to the supplicant device.
VLAN ID	The VLAN ID assigned by the authenticator to the supplicant device.
VLAN Assigned	The reason for the VLAN ID assigned by the authenticator to the supplicant device.
Session Timeout	The session time-out imposed by the RADIUS server on the supplicant device.
Termination Action	The termination action imposed by the RADIUS server on the supplicant device.

Set Up Traffic Control

You can configure MAC filters, storm control, port security, and protected port settings.

Manage MAC Filtering

You can create MAC filters that limit the traffic allowed into and out of specified ports on the switch.

Create a MAC Filter

If a packet with a MAC address and VLAN ID that you specify for a filter is received on a port that is not part of the inbound filter, the packet is dropped.

A packet with a MAC address and VLAN ID that you specify for a filter can be transmitted only from a port that is part of the outbound filter.

To create a MAC filter:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

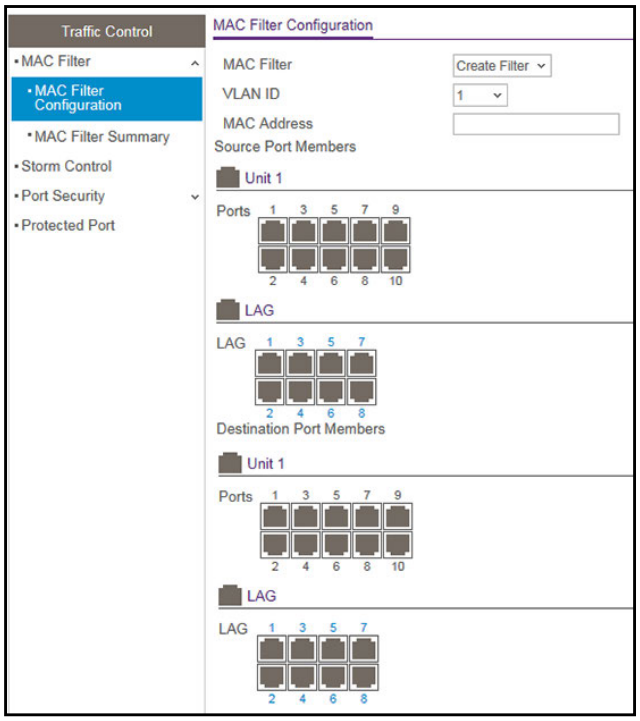
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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 previous figure shows the MAC Filter Configuration page for model GS310TP.

6. From the **MAC Filter** menu, select **Create Filter**.

   If you did not configure any filters, this is the only option available.

7. From the **VLAN ID** menu, select the VLAN that must be used with the MAC address.
8. In the **MAC Address** field, specify the MAC address of the filter in the format XX:XX:XX:XX:XX:XX.

   You cannot define filters for the following MAC addresses:

   - 00:00:00:00:00:00
   - 01:80:C2:00:00:00 to 01:80:C2:00:00:0F
   - 01:80:C2:00:00:20 to 01:80:C2:00:00:21
   - FF:FF:FF:FF:FF:FF

9. In the Port and LAG tables in the Source Port Members section, select the ports and LAGs that must be included in the inbound filter.

   If a packet with the MAC address and VLAN ID that you specify is received on a port that is not part of the inbound filter, the packet is dropped.

10. In the Port and LAG tables in the Destination Port Members section, select the ports and LAGs that must be included in the outbound filter.

    A packet with the MAC address and VLAN ID that you specify can be transmitted only from a port that is part of the outbound filter.

Note: Destination ports can be included only in a multicast filter. A multicast filter is determined by the MAC address that you enter in the **MAC Address** field.

11. Click the **Apply** button.

    Your settings are saved.

Delete a MAC FIlter

To delete a MAC filter:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Security > Traffic Control > MAC Filter > MAC Filter Configuration**.

   The MAC Filter Configuration page displays.
6. From the **MAC Filter** menu, select the filter.
7. Click the **Delete** button.

   The filter is removed.

MAC Filter Summary

You can view the MAC filters that are configured on the switch.

To view the MAC filter summary:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

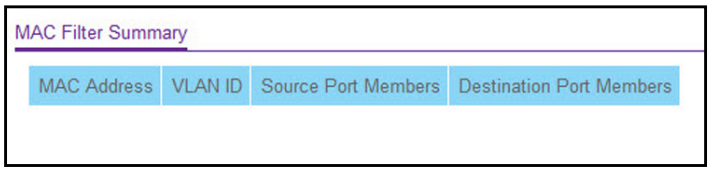
   The login window opens.

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.**



The following table describes the information displayed on the page.

Table 52. 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	The ports to be used for filtering inbound packets.
Destination Port Members	The ports to be used for filtering outbound packets.

Configure Storm Control Settings

A broadcast storm is the result of an excessive number of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses can overload network resources, cause the network to time out, or do both.

The switch measures the incoming packet rate per port for broadcast, multicast, unknown, and unicast packets and discards packets if the rate exceeds the defined value. You enable storm control per interface, by defining the packet type and the rate at which the packets are transmitted.

Configure Global Storm Control Settings

The global storm control settings apply to all ports. After you configure the global settings, you can specify storm control settings for one or more ports.

To configure global storm control settings:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

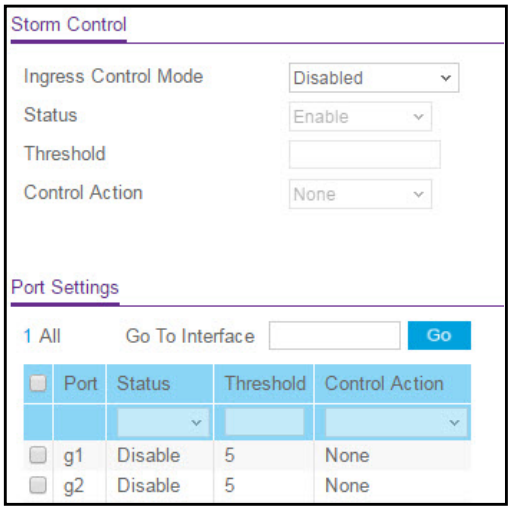
   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Traffic Control > Storm Control**.



6. In the Storm Control section, from the **Ingress Control Mode** menu, select one of the following modes for storm control:
   - **Disabled**. Storm control is disabled. This is the default setting.
   - **Unknown Unicast**. If the rate of incoming unknown Layer 2 unicast traffic (that is, traffic for which a destination lookup failure occurs) increases beyond the configured threshold on an interface, the traffic is dropped.
   - **Multicast**. If the rate of incoming Layer 2 multicast traffic increases beyond the configured threshold on an interface, the traffic is dropped.
   - **Broadcast**. If the rate of incoming Layer 2 broadcast traffic increases beyond the configured threshold on an interface, the traffic is dropped.

7. If the selection from the **Ingress Control Mode** menu is *not* **Disabled**, specify whether the ingress control mode is enabled by selecting **Enable** or **Disable** from the **Status** menu.
8. In the **Threshold** field, specify the maximum rate at which unknown packets are forwarded.

   The range is a percent of the total threshold between 0 and 100%. The default is 5%.
9. From the **Control Action** mode menu, select one of the following options:
   - **None**. No action is taken. This is the default setting.
   - **Trap**. If the threshold of the configured broadcast storm is exceeded, a trap is sent.
   - **Shutdown**. If the threshold of the configured broadcast storm is exceeded, the port is shut down.
10. Click the **Apply** button.

    Your settings are saved.

Configure Storm Control Settings for One or More Ports

After you configure the global settings, you can specify storm control settings for one or more ports.

To configure storm control settings for one or more ports:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

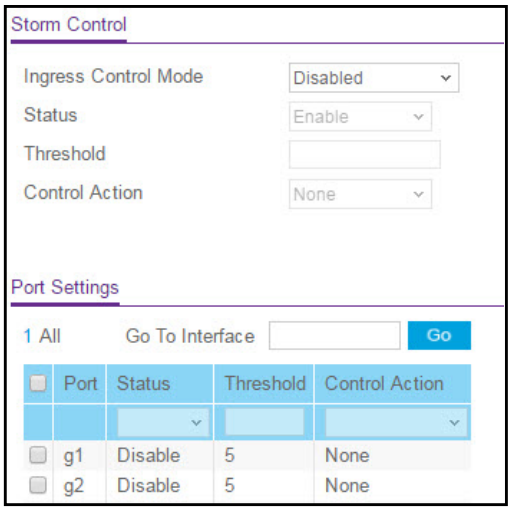
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Security > Traffic Control > Storm Control**.



The default settings in the Port Settings section depends on the global storm control settings (see Configure Global Storm Control Settings on page 242), which apply to all ports.

6. In the Port Settings section, select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
7. From the **Status** menu, specify whether the ingress control mode is enabled for the port by selecting **Enable** or **Disable**.
8. In the **Threshold** field, specify the maximum rate at which unknown packets are forwarded for the port.

   The range is a percent of the total threshold between 0 and 100%.
9. From the **Control Action** mode menu, select one of the following options for the port:
   - **None**. No action is taken.
   - **Trap**. If the threshold of the configured broadcast storm is exceeded, a trap is sent.
   - **Shutdown**. If the threshold of the configured broadcast storm is exceeded, the port is shut down.
10. Click the **Apply** button.

    Your settings are saved.

Manage Port Security

Port security lets you lock one or more ports on the switch. When a port is locked, the port can only forward packets with a source MAC addresses that you specifically allowed. The port discards all other packets.

Configure the Global Port Security Mode

To configure the global port security mode:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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.

   The page also shows the Port Security Violations table.

6. To enable port security on the switch, select the Port Security Mode **Enable** radio button.

   The default is Disable.

7. Click the **Apply** button.

   Your settings are saved.

   By default, port security is disabled for individual ports.

8. After you enable port security for individual ports (see Configure a Port Security Interface on page 247), click the **Update** button to refresh the page with the latest information about the ports.

The Port Security Violations table shows information about violations that occurred on ports that are enabled for port security.

The following table describes the fields in the Port Security Violations table.

Table 53. 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 allowed on a port by one of two methods: dynamically or statically. Both methods can be concurrently when a port is locked.

Dynamic locking implements a first arrival mechanism for port security. You specify how many addresses can be learned on the locked port. If the limit is not reached, a packet with an unknown source MAC address is learned and forwarded normally. If the limit is reached, no more addresses are learned on the port. Any packets with source MAC addresses that were not already learned are dropped. You can effectively disable dynamic locking by setting the number of allowable dynamic entries to zero.

Static locking allows you to specify a list of MAC addresses that are allowed on a port. The behavior of packets is the same as for dynamic locking: only packets with an allowable source MAC address can be forwarded.

To configure a port security interface:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

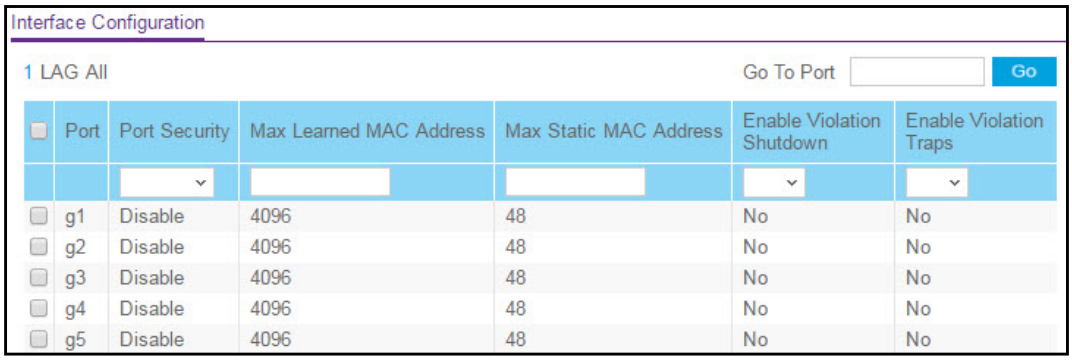
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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**.



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. The default is 4096.
   - **Max Static MAC Address**. Specify the maximum number of statically locked MAC addresses on the selected interfaces. The default is 48.
   - **Enable Violation Shutdown**. Enable or disable shutdown of the selected interfaces if a packet with a disallowed MAC address is received. The default value is No, which means that the option is disabled.
   - **Enable Violation Traps**. Enable or disable the sending of new violation traps if a packet with a disallowed MAC address is received. The default value is No, which means that the option is disabled.
8. Click the **Apply** button.

   Your settings are saved.

View Learned MAC Addresses and Convert Them to Static MAC Addresses

After you enabled port security globally (see Configure the Global Port Security Mode on page 246) and enabled port security for specific interfaces (see Configure a Port Security Interface on page 247), you can convert a dynamically learned MAC address to a statically locked address.

To view learned MAC addresses for an individual interface or LAG and convert these MAC addresses to static MAC addresses:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

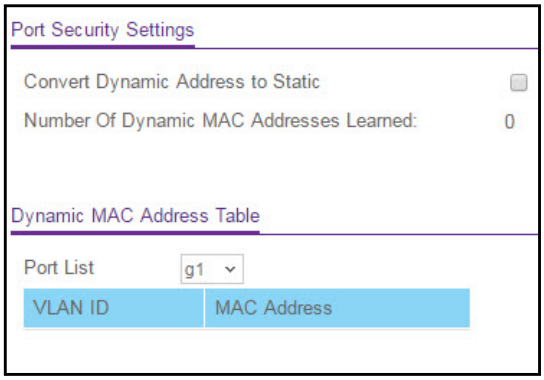
   The login window opens.

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 > Security MAC Address**.



6. From the **Port List** menu, select the individual interface.

   Port security must be enabled on the selected interface.

   The Dynamic MAC Address Table displays the MAC addresses and their associated VLANs that were learned on the selected port.

Field	Description
VLAN ID	The VLAN ID corresponding to the MAC address.
MAC Address	The MAC addresses learned on a specific port.

7. To convert the dynamically learned MAC address to a statically locked addresses, select the **Convert Dynamic Address to Static** check box.

8. Click the **Apply** button.

   The dynamic MAC address entries are converted to static MAC address entries in a numerically ascending order until the static limit is reached.

   The Number of Dynamic MAC Addresses Learned field displays the number of dynamically learned MAC addresses on a specific port.

9. To refresh the page with the latest information about the switch, click the **Update** button.

Configure Protected Ports

If you configure a port as protected, it does not forward traffic to any other protected port on the switch, but it does forward traffic to unprotected ports. You can configure the ports as protected or unprotected.

To configure protected ports:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

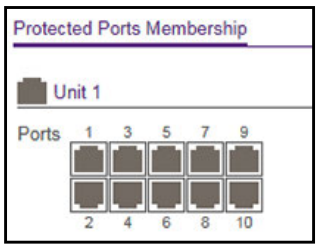
   The login window opens.

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**.



   The previous figure shows the Protected Ports Membership page for model GS310TP.

6. In the Ports table, click each port that you want to configure as a protected port.

Protected ports are marked with a check mark. No traffic forwarding is possible between two protected ports.

7. Click the **Apply** button.

   Your settings are saved.

Configure Access Control Lists

Access control lists (ACLs) ensure that only authorized users can access specific resources while blocking any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents, decide which types of traffic are forwarded or blocked, and provide security for the network. You can configure IPv4 and MAC ACLs.

To configure an ACL:

1. Create an IPv4-based or MAC-based ACL ID.
2. Create a rule and assign it to a unique ACL ID.
3. Define the rules, which can identify protocols, source, and destination IP and MAC addresses, and other packet-matching criteria.
4. Use the ID number to assign the ACL to a port or to a LAG.

To view ACL configuration examples, see Access Control Lists (ACLs) on page 335.

Use the ACL Wizard to Create a Simple ACL

The ACL Wizard helps you create a simple ACL and apply it to the selected ports easily and quickly. First, select an ACL type to use when you create an ACL. Then add an ACL rule to this ACL and apply this ACL on the selected ports. The ACL Wizard allows you to create the ACL, but does not allow you to modify it. To modify the ACL, go to the ACL Configuration page. See Configure a Basic or Extended IP ACL on page 266.

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.

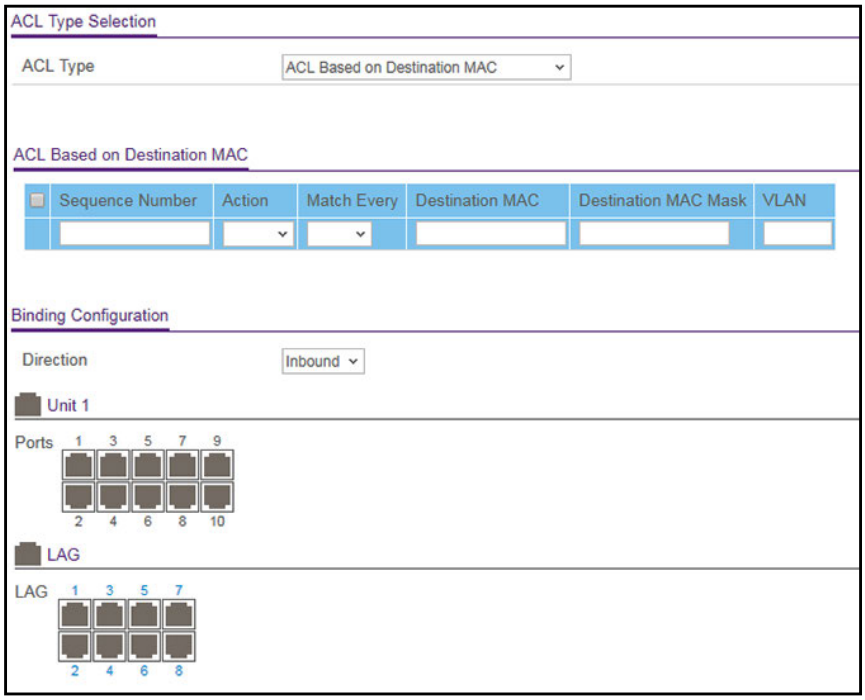
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Security > ACL > ACL Wizard**.



   The previous figure shows the ACL Wizard for model GS310TP.
6. From the **ACL Type** menu, select the type of ACL.

   You can select from the following ACL types:

   - **ACL Based on Destination MAC**. Creates an ACL based on the destination MAC address, destination MAC mask, and VLAN.
   - **ACL Based on Source MAC**. Creates an ACL based on the source MAC address, source MAC mask, and VLAN.
   - **ACL Based on Destination IPv4**. Creates an ACL based on the destination IPv4 address and IPv4 address mask.

- **ACL Based on Source IPv4**. Creates an ACL based on the source IPv4 address and IPv4 address mask.
- **ACL Based on Destination IPv4 L4 Port**. Creates an ACL based on the destination IPv4 Layer 4 port number.
- **ACL Based on Source IPv4 L4 Port**. Creates an ACL based on the source IPv4 Layer 4 port number.

Note: For L4 port options, two rules are created (one for TCP and one for UDP).

7. In the **Sequence Number** field, enter a whole number in the range from 1 to 2147483647 that is used to identify the rule.
8. From the **Action** menu, select **Permit** or **Deny** to specify the action that must be taken if a packet matches the rule's criteria.
9. From the **Match Every** menu, select one of the following options:
   - **False**. Packets do not need to match the selected ACL and rule. With this selection, you can add a destination MAC address, destination MAC mask, and VLAN.
   - **True**. All packets must match the selected ACL and rule and are either permitted or denied. In this case, since all packets match the rule, the option of configuring other match criteria is not offered.
10. Specify the additional match criteria for the selected ACL type.

    The rest of the rule match criteria fields available for configuration depend on the selected ACL type. For information about the possible match criteria fields, see the following table.

ACL Based On	Fields
Destination MAC	• **Destination MAC**. Specify the destination MAC address to compare against an Ethernet frame. The format is xx:xx:xx:xx:xx:xx. The BPDU keyword might be specified using a destination MAC address of 01:80:C2:xx:xx:xx. • **Destination MAC Mask**. Specify the destination MAC address mask, which represents the bits in the destination MAC address to compare against an Ethernet frame. The format is xx:xx:xx:xx:xx:xx. The BPDU keyword might be specified using a destination MAC mask of 00:00:00:ff:ff:ff. • **VLAN**. Specify the VLAN ID to match within the Ethernet frame.
Source MAC	• **Source MAC**. Specify the source MAC address to compare against an Ethernet frame. The format is xx:xx:xx:xx:xx:xx. • **Source MAC Mask**. Specify the source MAC address mask, which represents the bits in the source MAC address to compare against an Ethernet frame. The format is (xx:xx:xx:xx:xx:xx). • **VLAN**. Specify the VLAN ID to match within the Ethernet frame.
Destination IPv4	• **Destination IP Address**. Specify the destination IP address. • **Destination IP Mask**. Specify the destination IP address mask.
Source IPv4	• **Source IP Address**. Specify the source IP address. • **Source IP Mask**. Specify the source IP address mask.

ACL Based On	Fields
Destination IPv4 L4 Port	• **Destination L4 port (protocol)**. Specify the destination IPv4 L4 port protocol. • **Destination L4 port (value)**. Specify the destination IPv4 L4 port value.
Source IPv4 L4 Port	• **Source L4 port (protocol)**. Specify the source IPv4 L4 port protocol. • **Source L4 port (value)**. Specify the source IPv4 L4 port value.

11. As a sample, the following steps describe how you can create an ACL based on the destination MAC address:

a. In the **Destination MAC** field, specify the destination MAC address that must be compared against the information in an Ethernet frame.

The 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 format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC mask of 00:00:00:ff:ff:ff.

c. In the **VLAN ID** field, specify which VLAN must be compared against the information in an Ethernet frame.

The range is from 1 to 4093. Either a VLAN range or VLAN can be configured.

12. In the Binding Configuration section, from the **Direction** menu, select the packet filtering direction for the ACL.

Only the inbound direction is valid.

13. In the Ports and LAG tables in the Binding Configuration section, select the ports and LAGs to which the ACL must be applied.

14. Click the **Add** button.

The rule is added to the ACL.

15. Click the **Apply** button.

Your settings are saved.

Modify an ACL Rule

To modify an ACL rule:

1. Connect your computer to the same network as the switch.

You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > ACL Wizard**.

   The ACL Wizard page displays.

6. Select check box that is associated with the rule.
7. Update the match criteria as needed.
8. Click the **Apply** button.

   Your settings are saved.

Delete an ACL Rule

To delete an ACL rule:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > ACL Wizard**.

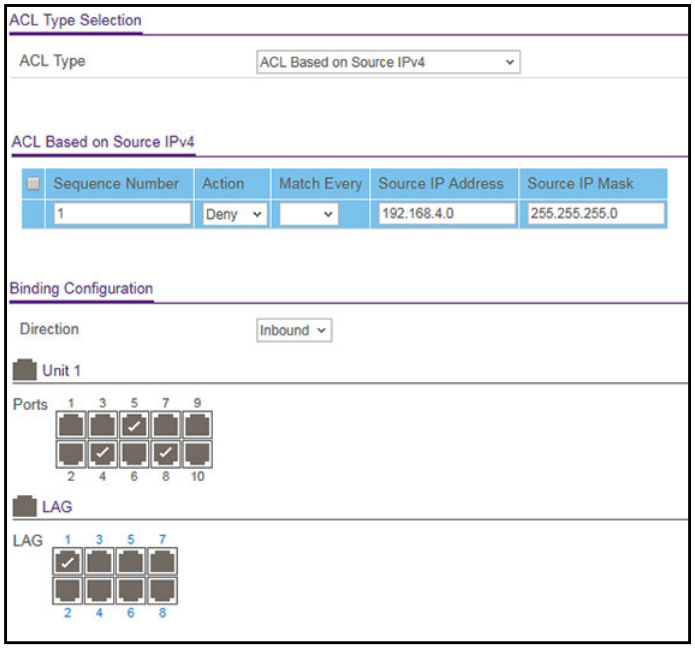
   The ACL Wizard page displays.

6. Select check box that is associated with the rule.
7. Click the **Delete** button.

   The rule is removed.

ACL Wizard Example

In the following figure, the ACL rule is configured to check for packet matches on ports 4, 5, and 9 and on LAG 1. Only the Inbound option is valid. Packets that include a source address in the 192.168.4.0/16 network are permitted to be forwarded by the interfaces. All other packets are dropped because every ACL includes an implicit *deny all* rule as the last rule.



The previous figure shows a sample for model GS310TP.

For information about the ACL Wizard, see Use the ACL Wizard to Create a Simple ACL on page 251.

Configure a Basic MAC ACL

A MAC ACL consists of a set of rules that are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit or Deny) is taken, and the additional rules are not checked for a match.

Multiple steps are involved in defining a MAC ACL and applying it to the switch:

1. Create a MAC ACL ID (see Add a MAC ACL on page 257).
2. Create a MAC rule (see Configure MAC ACL Rules on page 259).
3. Associate the MAC ACL with one or more interfaces (see Configure MAC Bindings on page 263).

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 265.

Add a MAC ACL

To add a MAC ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

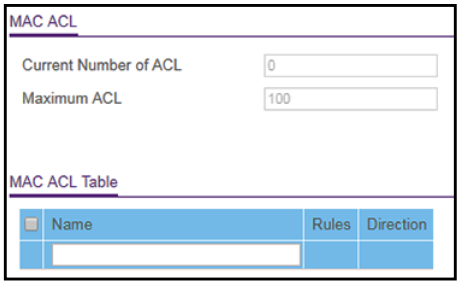
   The login window opens.

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 Table displays the number of ACLs currently configured in the switch and the maximum number of ACLs that can be configured. The current size is equal to the number of configured IPv4 plus the number of configured MAC ACLs.

6. In the **Name** field, specify a name for the MAC ACL.

   The name string can include alphabetic, numeric, hyphen, underscore, or space characters only. The name must start with an alphabetic character.

7. Click the **Add** button.

   The MAC ACL is added.

   Each configured ACL displays the following information:

   - **Rules**. The number of rules currently configured for the MAC ACL.
   - **Direction**. The direction of packet traffic affected by the MAC ACL, which can be Inbound or blank. (If the ACL is not bound to an interface, the direction is blank.)

Change the Name of a MAC ACL

To change the name of a MAC ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Security > ACL > Basic > MAC ACL**.

   The MAC ACL page displays.
6. Select check box that is associated with the MAC ACL.
7. In the **Name** field, specify the new name.
8. Click the **Apply** button.

   Your settings are saved.

Delete a MAC ACL

To delete a MAC ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

The default password is **password**.

The System Information page displays.

5. Select **Security > ACL > Basic > MAC ACL**.

   The MAC ACL page displays.

6. Select check box that is associated with the MAC ACL.
7. Click the **Delete** button.

   The MAC ACL is removed.

Configure MAC ACL Rules

You can define rules for MAC-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. A default *deny all* rule is the last rule of every list.

Add a Rule to a MAC ACL

To add a rule to a MAC ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

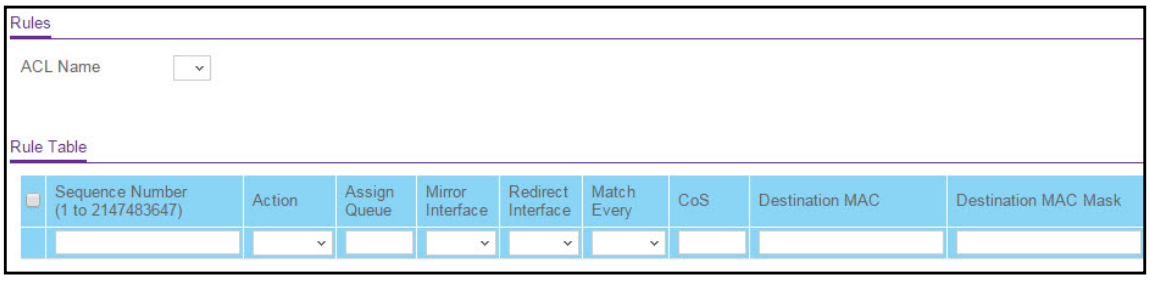
   The login window opens.

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 previous figure does not show all columns.

6. From the **ACL Name** menu, select the MAC ACL.
7. In the **Sequence Number** field, enter a whole number in the range from 1 to 2147483647 to identify the rule.
8. From the **Action** menu, select the action that must be taken if a packet matches the rule's criteria:
   - **Permit**. Forwards packets that meet the ACL criteria.
   - **Deny**. Drops packets that meet the ACL criteria.
9. In the **Assign Queue** field, specify the hardware egress queue identifier that must be used to handle all packets matching this ACL rule.

   The range for the queue ID is from 0 to 7.
10. From the **Mirror Interface** menu, select the specific egress interface to which the matching traffic stream must be copied, in addition to being forwarded normally by the switch.

    This field cannot be set if a redirect interface is already configured for the ACL rule. This field is visible for a Permit action.
11. From the **Redirect Interface** menu, select the egress interface to which the matching traffic stream must be redirected, bypassing any forwarding decision normally performed by the switch.

    This field cannot be set if a mirror interface is already configured for the ACL rule.
12. From the **Match Every** menu, select whether each Layer 2 MAC packet must be matched against the rule:
    - **True**. Each packet must match the selected ACL rule.
    - **False**. Not all packets need to match the selected ACL rule.
13. In the **CoS** field, specify the 802.1p user priority that must be compared against the information in an Ethernet frame.

    The range for the priority is from 0 to 7.
14. In the **Destination MAC** field, specify the destination MAC address that must be compared against the information in an Ethernet frame.

    The 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.
15. In the **Destination MAC Mask** field, specify the destination MAC address mask that must be compared against the information in an Ethernet frame.

    The format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC mask of 00:00:00:ff:ff:ff.
16. From the **EtherType Key** menu, select the EtherType value that must be compared against the information in an Ethernet frame.

The values are as follows:

- **Apple Talk**
- **IBM SNA**
- **IPv4**
- **IPX**
- **MPLS Multicast**
- **MPLS Unicast**
- **NetBios**
- **Novell**
- **PPPOE**
- **RARP**
- **User Value**

17. If you select **User Value** from the **EtherType Key** menu, in the **EtherType User Value** field, specify the customized EtherType value that must be used.

    This value must be compared against the information in an Ethernet frame. The range is from 0x0600 to 0xFFFF.

18. In the **Source MAC** field, specify the source MAC address that must be compared against the information in an Ethernet frame.

    The format is xx:xx:xx:xx:xx:xx.

19. In the **Source MAC Mask** field, specify the source MAC address mask that must be compared against the information in an Ethernet frame.

    The format is xx:xx:xx:xx:xx:xx.

20. In the **VLAN** field, specify the VLAN ID that must be compared against the information in an Ethernet frame.

    The range is from 1 to 4095. Either VLAN range or VLAN can be configured.

21. From the **Logging** menu, select whether to enable or disable logging.

    If you select **Enable**, logging is enabled for this ACL rule (subject to resource availability on the switch).

22. Click the **Add** button.

    The rule is added.

Change the Match Criteria for a MAC Rule

To change the match criteria for a MAC rule:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.

3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Basic > MAC Rules**.

   The MAC Rules page displays.

6. Select the check box that is associated with the rule.
7. Modify the fields as needed.
8. Click the **Apply** button.

   Your settings are saved.

Delete a Rule for a MAC ACL

To delete a rule for a MAC:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Basic > MAC Rules**.

   The MAC Rules page displays.

6. Select the check box that is associated with the rule.

7. Click the **Delete** button.

   The rule is removed.

Configure MAC Bindings

When an ACL is bound to an interface, all the rules that are defined are applied to the selected interface. You can assign MAC ACLs lists to interfaces and LAGs.

To configure MAC bindings:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

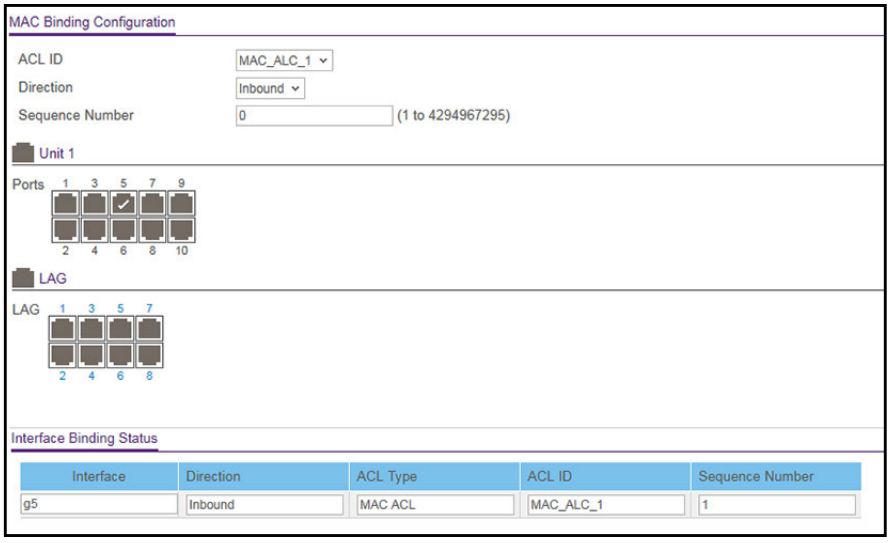
   The login window opens.

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 previous figure shows the MAC Binding Configuration page for model GS310TP.

6. From the **ACL ID** menu, select an ACL.

   The fixed selection from the **Direction** menu is **Inbound**, which means that MAC ACL rules are applied to traffic entering the interface.

7. In the **Sequence Number** field, optionally specify a number to indicate the order of the access list relative to other access lists already assigned to the interface and direction.

   A low number indicates high precedence order. If a sequence number is already in use for the interface and direction, the specified access list replaces the currently attached access list using that sequence number. If you do not specify the sequence number, a sequence number that is one number greater than the highest sequence number currently in use for the interface and direction is used. The range is from 1 to 4294967295.

8. To add the selected ACL to a port or LAG, in the Ports table or LAG table, click the port or LAG so that a check mark displays.

   You can add the ACL to several ports and LAGs.

   The Ports and LAG tables display the available interfaces for ACL bindings. All nonrouting physical interfaces, VLAN interfaces, and interfaces participating in LAGs are listed.

9. Click the **Apply** button.

   Your settings are saved.

The following table describes the information displayed in the Interface Binding Status table.

Table 54. 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 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.

View or Delete MAC ACL Bindings in the MAC Binding Table

You can view or delete the MAC ACL bindings in the MAC Binding Table.

To view or delete MAC ACL bindings:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

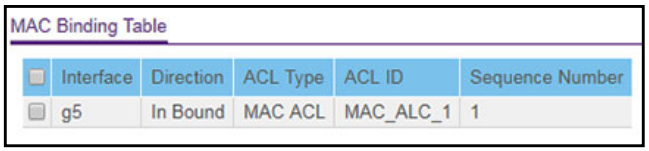
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Security > ACL > Basic > MAC Binding Table**.



6. To delete a MAC ACL-to-interface binding, do the following:
   a. Select the check box next to the interface.
   b. Click the **Delete** button.

   The binding is removed.

The following table describes the information that is displayed in the MAC Binding Table.

Table 55. 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.

Table 55. MAC Binding Table (continued)

Field	Description
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 a Basic or Extended IP ACL

An IP ACL consists of a set of rules that are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit or Deny) is taken, and the additional rules are not checked for a match. You must specify the interfaces to which an IP ACL applies, as well as whether it applies to inbound or outbound traffic.

Multiple steps are involved in defining an IP ACL and applying it to the switch:

1. Add an IP ACL ID (see Add an IP ACL on page 266).

   The differences between a basic IP ACL and an extended IP ACL are as follows:

   - **Numbered ACL from 1 to 99**. Creates a basic IP ACL, which allows you to permit or deny traffic from a source IP address.
   - **Numbered ACL from 100 to 199**. Creates an extended IP ACL, which allows you to permit or deny specific types of Layer 3 or Layer 4 traffic from a source IP address to a destination IP address. This type of ACL provides more granularity and filtering capabilities than the basic IP ACL.
   - **Named IP ACL**. Create an extended IP ACL with a name string that is up to 31 alphanumeric characters in length. The name must start with an alphabetic character.
2. Create an IP rule (see Configure Rules for a Basic IP ACL on page 269 or Configure Rules for an Extended IP ACL on page 273).
3. Associate the IP ACL with one or more interfaces (see Configure IP ACL Interface Bindings on page 280).

You can view or delete IP ACL configurations in the IP ACL Binding table (see View or Delete IP ACL Bindings in the IP ACL Binding Table on page 282.

Add an IP ACL

To add an IP ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

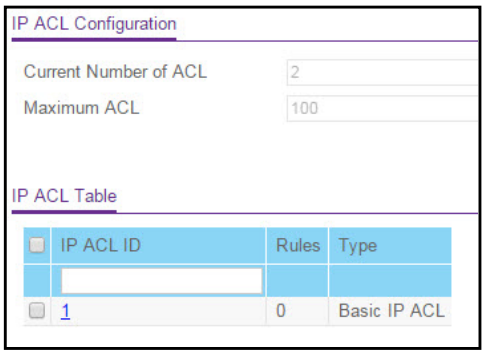
The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Advanced > IP ACL**.



   The IP ACL page shows the current size of the ACL table compared to the maximum size of the ACL table. The current size is equal to the number of configured IPv4 ACLs plus the number of configured MAC ACLs. The maximum size is 100.

   The Current Number of ACL field displays the current number of all ACLs configured on the switch.

   The Maximum ACL field displays the maximum number of IP ACLs that can be configured on the switch.

6. In the **IP ACL ID** field, specify the ACL ID or IP ACL name, which depends on the IP ACL type. The IP ACL ID is an integer in the following range:
   - **1–99**. Creates a basic IP ACL, which allows you to permit or deny traffic from a source IP address.
   - **100–199**. Creates an extended IP ACL, which allows you to permit or deny specific types of Layer 3 or Layer 4 traffic from a source IP address to a destination IP address. This type of ACL provides more granularity and filtering capabilities than the standard IP ACL.
   - **IP ACL Name**. Create an extended IP ACL with a name string that is up to 31 alphanumeric characters in length. The name must start with an alphabetic character.

   Each configured ACL displays the following information:

   - **Rules**. The number of rules currently configured for the IP ACL.
   - **Type**. Identifies the ACL as a basic IP ACL (with ID from 1 to 99), extended IP ACL (with ID from 100 to 199 or a name).

7. Click the **Add** button.

   The IP ACL is added.

Change the Name of an IP ACL

To change the name of an IP ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Security > ACL > Advanced > IP ACL**.

   The IP ACL Configuration page displays.
6. Select the check box that is associated with the IP ACL.
7. In the **IP ACL** field, specify the new name.
8. Click the **Apply** button.

   Your settings are saved.

Delete an IP ACL

To delete an IP ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Advanced > IP ACL**.

   The IP ACL Configuration page displays.

6. Select the check box that is associated with the IP ACL.
7. Click the **Delete** button.

   The IP ACL is removed.

Configure Rules for a Basic IP ACL

You can define rules for IP-based standard ACLs (basic ACLs). The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

Note: An implicit *deny all* rule is included at the end of an ACL list. This means that if an ACL is applied to a packet, and if none of the explicit rules match, then the final implicit *deny all* rule applies and the packet is dropped.

Add a Rule for a Basic IP ACL

To add a rule for a basic IP ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

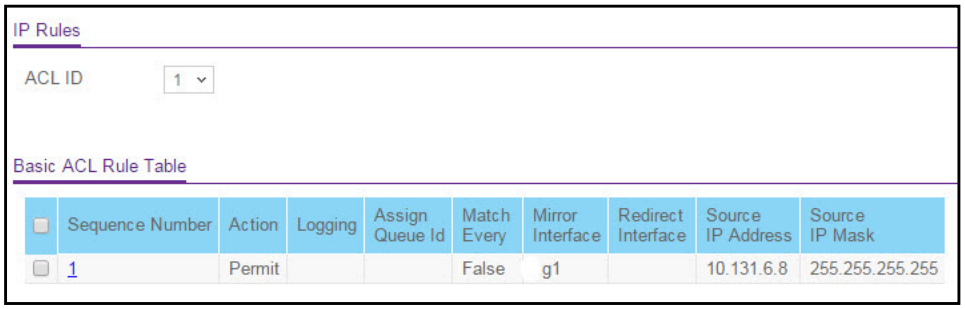
   The login window opens.

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**.

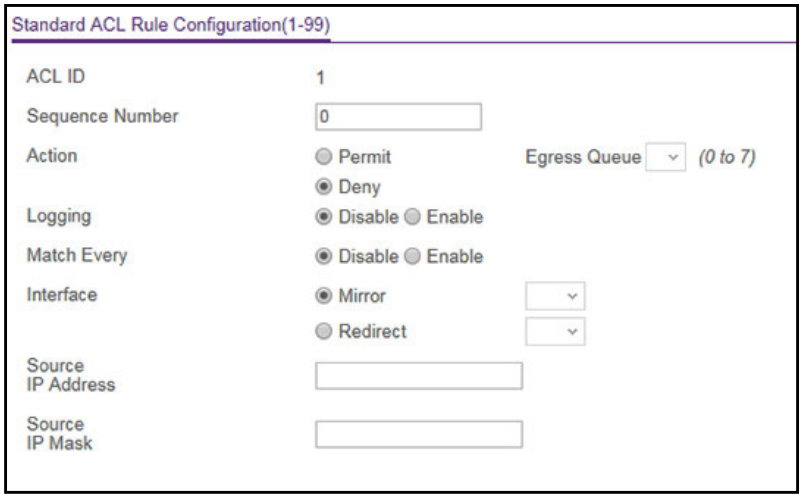


If no rules exist, the Basic ACL Rule Table shows the message *No rules have been configured for this ACL*. If one or more rules exist for the ACL, the rules display in the Basic ACL Rule Table.

6. From the **ACL ID** menu, select the IP ACL for which you want to add a rule.

   For basic IP ACLs, this must be an ID in the range from 1 to 99.

7. Click the **Add** button.



8. Specify the following match criteria for the rule:
   - **Sequence Number**. Enter an ACL sequence number in the range from 1 to 2147483647 that is used to identify the rule. An IP ACL can contain up to 50 rules.
   - **Action**. Select the ACL forwarding action, which is one of the following:
     - **Permit**. Forward packets that meet the ACL criteria.

       Egress Queue. If the selection form the **Action** menu is **Permit**, you can specify the hardware egress queue identifier that is used to handle all packets matching this IP ACL rule. The range of queue IDs is from 0 to 7.

     - **Deny**. Drop packets that meet the ACL criteria.

Logging. If the selection from the **Action** menu is **Deny**, you can enable logging for the ACL by selecting the **Enable** radio button. (Logging is subject to resource availability on the switch.)

- **Match Every**. Select one of the radio buttons to specify whether all packets must match the selected IP ACL rule:
  - **Enable**. All packets must match the selected IP ACL rule and are either permitted or denied.
  - **Disable**. Not all packets need to match the selected IP ACL rule.
- **Interface**. Select one of the radio buttons to specify whether all packets must be mirrored or redirected:
  - **Mirror**. From the menu, select the specific egress interface to which the matching traffic stream must be copied, in addition to being forwarded normally by the switch.
  - **Redirect**. From the menu, select the egress interface to which the matching traffic stream must be redirected, bypassing any forwarding decision normally performed by the switch.
- **Source 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.
- **Source IP Mask**. Specify the IP mask in dotted-decimal notation to be used with the source IP address value.

9. Click the **Apply** button.

   Your settings are saved.

Modify the Match Criteria for a Basic IP ACL Rule

To modify the match criteria for a basic IP ACL rule:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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.

   Your settings are saved.

Delete a Basic IP ACL Rule

To delete a basic IP ACL rule:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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 matching the criteria is forwarded normally or discarded.

Note: An implicit *deny all* rule is included at the end of an ACL list. This means that if an ACL is applied to a packet and if none of the explicit rules match, then the final implicit *deny all* rule applies and the packet is dropped.

Add a Rule for an Extended IP ACL

To add a rule for an extended IP ACL:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

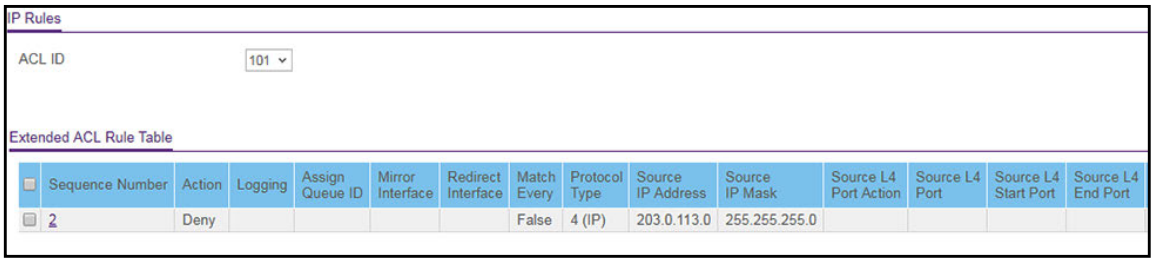
   The login window opens.

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**.



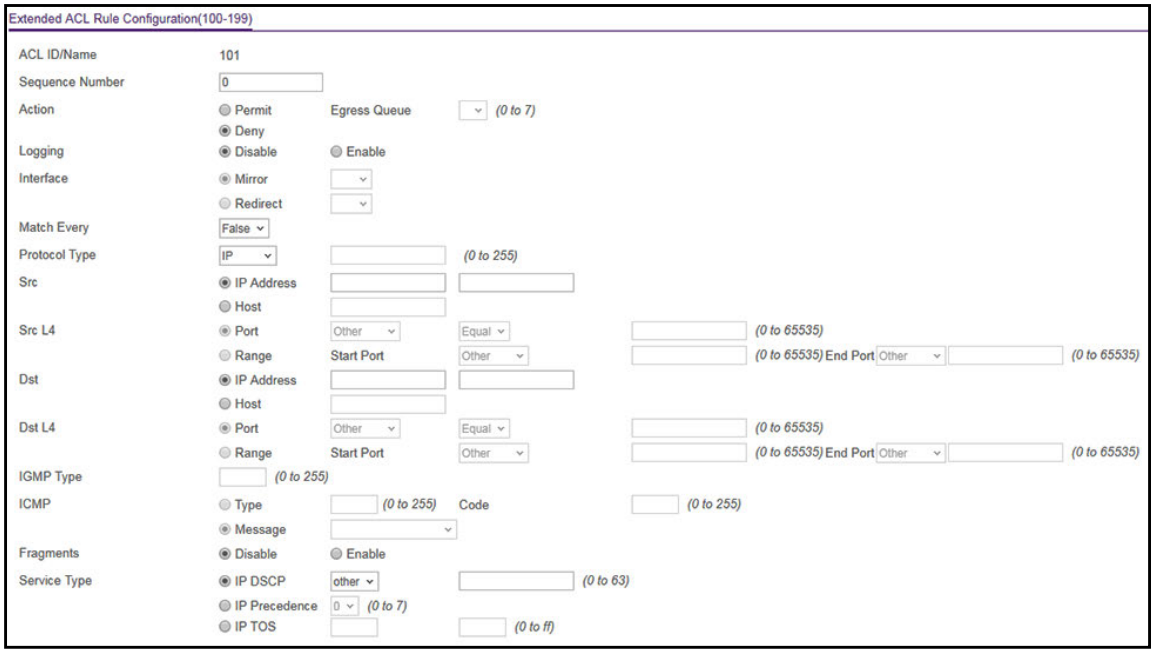
   The previous figure does not show all columns on the page.

   If no rules exists, the Extended ACL Rule Table shows the message *No rules have been configured for this ACL*. If one or more rules exist for the ACL, the rules display in the Extended ACL Rule Table.

6. From the **ACL ID** menu, select the IP ACL for which you want to add a rule.

   For extended IP ACLs, this must be an ID in the range from 101 to 199 or a name.

7. Click the **Add** button.



8. Configure the following match criteria for the rule:
   - **Sequence Number**. Enter a number in the range from 1 to 2147483647 that is used to identify the rule. An extended IP ACL can contain up to 50 rules.
   - **Action**. Select the ACL forwarding action, which is one of the following:
     - **Permit**. Forward packets that meet the ACL criteria.

       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.

     - **Deny**. Drop packets that meet the ACL criteria.

       Logging. If the selection form 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.)

   - **Interface**. For a Permit action, use either a mirror interface or a redirect interface:
     - Select the **Mirror** radio button and use the menu to specify the egress interface to which the matching traffic stream is copied, in addition to being forwarded normally by the device.
     - Select the **Redirect** radio button and use the menu to specify the egress interface to which the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device.

- **Match Every**. Select one of the radio buttons to specify whether all packets must match the selected IP ACL rule:
  - **False**. Not all packets need to match the selected IP ACL rule. You can configure other match criteria on the page.
  - **True**. All packets must match the selected IP ACL rule and are either permitted or denied. In this case, you cannot configure other match criteria on the page.
- **Protocol Type**. From the menu, select a protocol that a packet's IP protocol must be matched against: **IP**, **ICMP**, **IGMP**, **TCP**, **UDP**, **EIGRP**, **GRE**, **IPINIP**, **OSPF**, **PIM**, or **Other**. If you select **Other**, enter a protocol number from 0 to 255.
- **Src**. In the **Src** field, enter a source IP address, using dotted-decimal notation, to be compared to a packet's source IP address as a match criterion for the selected IP ACL rule:
  - If you select the **IP Address** radio button, enter an IP address or an IP address range. You can enter a relevant wildcard mask to apply this criteria. If this field is left empty, it means *any*.
  - If you select the **Host** radio button, the wildcard mask is configured as 0.0.0.0. If this field is left empty, it means *any*.

  The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard of 255.255.255.255 indicates that *all* of the bits are important.
- **Src L4**. The options are available only when the protocol is set to TCP or UDP. Use the source L4 port option to specify relevant matching conditions for L4 port numbers in the extended ACL rule.

  You can select either the **Port** radio button or the **Range** radio button:

  - If you select the **Port** radio button, you can either enter the port number yourself or select one of the following protocols from the menu:
    - The source IP TCP port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **www-http**, **smtp**, **telnet**, **pop2**, **pop3**, and **bgp**.
    - The source IP UDP port protocols are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **tftp**.

    Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

    Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.

    The only relevant matching condition for L4 port numbers is **Equal**. This means that an IP ACL rule matches only if the Layer 4 source port number is equal to the specified port number or port protocol.
  - If you select the **Range** radio button, the IP ACL rule matches only if the Layer 4 source port number is within the specified port range. The starting port, ending port, and all ports in between are a part of the Layer 4 port range.

The **Start Port** and **End Port** fields identify the first and last ports that are part of the port range. The values can range from 0 to 65535.

You can either enter the port range yourself or select one of the following protocols from the menu:

- The destination IP TCP port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **www-http**, **smtp**, **telnet**, **pop2**, **pop3**, and **bgp**.
- The destination IP UDP port protocols are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **tftp**.

Each of these values translates into its equivalent port number, which is used as both the start and end of the port range. Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.

The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard of 255.255.255.255 indicates that *all* of the bits are important.

- **Dst**. In the **Dst** field, enter a destination IP address, using dotted-decimal notation, to be compared to a packet's destination IP address as a match criterion for the selected IP ACL rule:
  - If you select the **IP Address** radio button, enter an IP address with a relevant wildcard mask to apply this criteria. If this field is left empty, it means *any*.
  - If you select the **Host** radio button, the wildcard mask is configured as 0.0.0.0. If this field is left empty, it means *any*.

  The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard of 255.255.255.255 indicates that *all* of the bits are important.
- **Dst L4**. The options are available only when the protocol is set to TCP or UDP. Use the destination L4 port option to specify relevant matching conditions for L4 port numbers in the extended ACL rule.

  You can select either the **Port** radio button or the **Range** radio button:

  - If you select the **Port** radio button, you can either enter the port number yourself or select one of the following protocols from the menu.
    - The destination IP TCP port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **www-http**, **smtp**, **telnet**, **pop2**, **pop3**, and **bgp**.
    - The destination IP UDP port protocols are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **tftp**.

    Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

    Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.

The only relevant matching condition for L4 port numbers is **Equal**. This means that an IP ACL rule matches only if the Layer 4 source port number is equal to the specified port number or port protocol.

- If you select the **Range** radio button, the IP ACL rule matches only if the Layer 4 destination port number is within the specified port range. The starting port, ending port, and all ports in between are a part of the Layer 4 port range.

  The **Start Port** and **End Port** fields identify the first and last ports that are part of the port range. They values can range from 0 to 65535.

  You can either select the enter the port range yourself or select one of the following protocols from the menu:

  - The destination IP TCP port range names are **domain**, **echo**, **ftp**, **ftpdata**, **www-http**, **smtp**, **telnet**, **pop2**, **pop3**, and **bgp**.
  - The destination IP UDP port range names are **domain**, **echo**, **snmp**, **ntp**, **rip**, **time**, **who**, and **tftp**.

  Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

  Select **Other** from the menu to enter a port number. If you select **Other** from the menu but leave the field blank, it means *any*.

  The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard of 255.255.255.255 indicates that *all* of the bits are important.

- **IGMP Type**. If your selection from the **Protocol Type** menu is **IGMP** and you specify the IGMP type, the IP ACL rule matches the specified IGMP message type. The range is from 0 to 255. If this field is left empty, it means *any*.
- **ICMP**. If your selection from the **Protocol Type** menu is **ICMP**, you can select either the **Type** or **Message** radio button:
  - If you select the **Type** radio button, note the following:
    - The **Type** and **Code** fields are enabled only if the protocol is ICMP. Use these fields to specify a match condition for ICMP packets:
    - If you specify information in the **Type** field, the IP ACL rule matches the specified ICMP message type. The type number can be from 0 to 255.
    - If you specify information in the **Code** field, the IP ACL rule matches the specified ICMP message code. The code can be from 0 to 255.
    - If these fields are left empty, it means *any*.
  - If you select the **Message** radio button, from the menu, select the type of the ICMP message to match with the selected IP ACL rule. Specifying a type of message implies that both the ICMP type and ICMP code are specified. The ICMP message is decoded into the corresponding ICMP type and ICMP code within the ICMP type.

    The IPv4 ICMP message types are **echo**, **echo-reply**, **host-redirect**, **mobile-redirect**, **net-redirect**, **net-unreachable**, **redirect**, **packet-too-big**,

port-unreachable, **source-quench**, **router-solicitation**, **router-advertisement**, **ttl-exceeded**, **time-exceeded**, and **unreachable**.

- **Fragments**. Either select the **Enable** radio button to allow initial fragments (that is, the fragment bit is asserted) or leave the default **Disable** radio button selected to prevent initial fragments from being used.

  This option is not valid for rules that match L4 information such as a TCP port number, because that information is carried in the initial packet.

- **Service Type**. Select a service type match condition for the extended IP ACL rule.

  The possible options are **IP DSCP**, **IP precedence**, and **IP TOS**, which are alternative methods to specify a match criterion for the same service type field in the IP header. Each method uses a different user notation. After you make a selection, you can specify the appropriate values:

  - **IP DSCP**. This is an optional configuration. Specify the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order 6 bits of the service type octet in the IP header. Enter an integer from 0 to 63. To select the IP DSCP, select one of the DSCP keywords from the menu. To specify a numeric value, select **Other** and a field displays in which you can enter numeric value of the DSCP.
  - **IP Precedence**. This is an optional configuration. The IP precedence field in a packet is defined as the high-order 3 bits of the service type octet in the IP header. Enter a number from 0 to 7.
  - **IP TOS**. This is an optional configuration. The IP ToS field in a packet is defined as all 8 bits of the service type octet in the IP header. The ToS bits value is a hexadecimal number that is composed of numbers 00 to 09 and AA to FF. The ToS mask value is a hexadecimal number that is composed of numbers 00 to FF. The ToS mask denotes the bit positions in the ToS bits value that are used for comparison against the IP ToS field in a packet.

    For example, to check for an IP ToS value for which bit 7 is set and is the most significant value, for which bit 5 is set, and for which bit 1 is cleared, use a ToS bits value of 0xA0 and a ToS mask of 0xFF.

9. Click the **Apply** button.

   Your settings are saved.

Modify the Match Criteria for an Extended IP ACL Rule

To modify the match criteria for an existing extended IP ACL rule:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Advanced > IP Extended Rules**.

   The IP Rules page displays.

6. From the **ACL ID** menu, select the ACL that includes the rule that you want to modify.
7. In the Extended ACL Rule Table, click the rule.

   The rule is a hyperlink. The Extended ACL Rule Configuration page displays.

8. Modify the extended IP ACL rule criteria.
9. Click the **Apply** button.

   Your settings are saved.

Delete an Extended IP ACL Rule

To delete an extended IP ACL rule:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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

When you bind an IP ACL to an interface, all the rules that you defined for the IP ACL are applied to the selected interface.

If resources on the switch are insufficient, an attempt to bind an ACL to an interface fails.

To bind an IP ACL to one or more interfaces:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

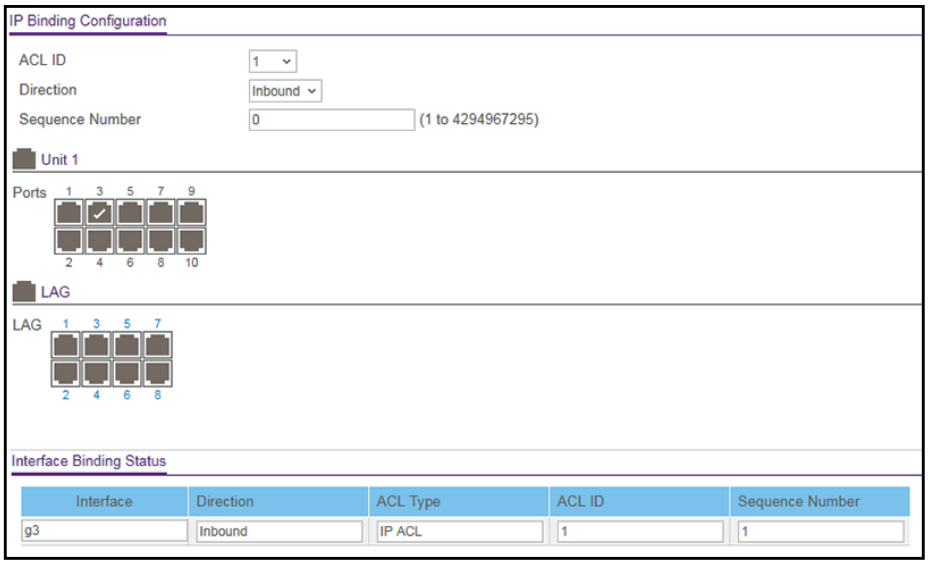
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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 previous figure shows the IP Binding Configuration page for model GS310TP.

6. From the **ACL ID** menu, select the 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 IP ACL rules are applied to traffic entering the interface.

7. In the **Sequence Number** field, optionally specify a number to indicate the order of the access list relative to other access lists already assigned to the interface and direction.

   A low number indicates high precedence order. If a sequence number is already in use for the interface and direction, the specified access list replaces the currently attached access list using that sequence number. If you do not specify the sequence number (meaning that the value is 0), a sequence number that is one number greater than the highest sequence number currently in use for the interface and direction is used. The range is from 1 to 4294967295.

8. To add the selected ACL to a port or LAG, in the Ports table or LAG table, click the port or LAG so that a check mark displays.

   You can add the ACL to several ports and LAGs.

   The Ports and LAG tables display the available interfaces for ACL bindings. All nonrouting physical interfaces, VLAN interfaces, and interfaces participating in LAGs are listed.

9. Click the **Apply** button.

   Your settings are saved.

The following table describes the nonconfigurable information displayed on the page.

Table 56. IP Binding Status table

Field	Description
Interface	The selected interface.
Direction	The selected packet filtering direction for the ACL, which is always Inbound.
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 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 IP ACL bindings.

To view or delete IP ACL bindings:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

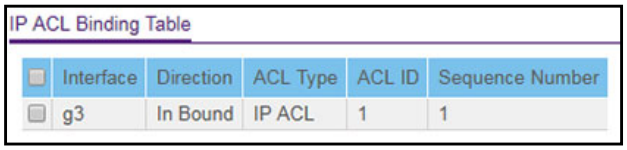
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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**.



6. To delete an IP ACL-to-interface binding, do the following:
   a. Select the check box next to the interface.

b. Click the **Delete** button.

The binding is removed.

The following table describes the information displayed in the IP ACL Binding Table.

Table 57. IP ACL Binding Table

Field	Description
Interface	The interface.
Direction	The selected packet filtering direction for the ACL, which is always Inbound.
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 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.

Configure VLAN ACL Bindings

You can associate a MAC ACL or IP ACL with a VLAN. When you do so, the ACL is applied to all interfaces that are members of the VLAN.

Add a VLAN ACL Binding

To add a VLAN ACL binding:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

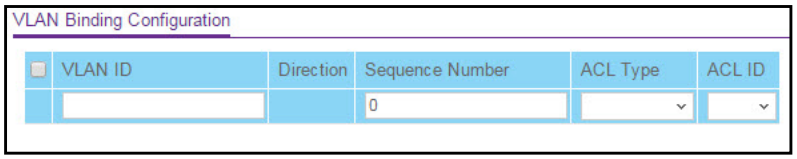
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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 > VLAN Binding Configuration**.



6. In the **VLAN ID** field, enter the VLAN ID to which the binding must apply.

   The direction for packet filtering is always inbound.

7. In the **Sequence Number** field, enter an optional sequence number.

   You can specify an optional sequence number to indicate the order of this access list relative to other access lists that are already assigned to the VLAN ID and selected direction. A lower number indicates a higher precedence order. If a sequence number is already in use for the VLAN ID and selected direction, the specified access list replaces the currently attached ACL using that sequence number. If you do not specify a sequence number (the value is 0), a sequence number that is one greater than the highest sequence number currently in use for the VLAN ID and selected direction is used.The range is from 1 to 4294967295.

8. From the **ACL Type** menu, select the type of ACL.

   You can select a MAC ACL or IP ACL.

9. From the **ACL ID** list, select the ID or name of the ACL that must be bound to the specified VLAN.
10. Click the **Add** button.

    The VLAN ACL binding is added.

Remove a VLAN ACL Binding

To remove a VLAN ACL binding:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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 > VLAN Binding Configuration**.

   The VLAN Binding Configuration page displays.
6. Select the check box for the VLAN binding that you want to remove.
7. Click the **Delete** button.

   The VLAN ACL binding is removed.

6

Monitor the System

This chapter contains the following sections:

- Monitor the Switch and the Ports
- Configure and View Logs
- Configure Port Mirroring

Monitor the Switch and the Ports

The following sections describe how you can view a variety of information about the amount and type of traffic that is transmitted from and received on the switch:

- View Switch Statistics on page 287
- View Port Statistics on page 290
- View and Manage Detailed Port Statistics on page 293
- View or Clear EAP and EAPoL Statistics on page 299
- Perform a Cable Test on page 300

View Switch Statistics

You can view detailed statistical information about the traffic that 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.

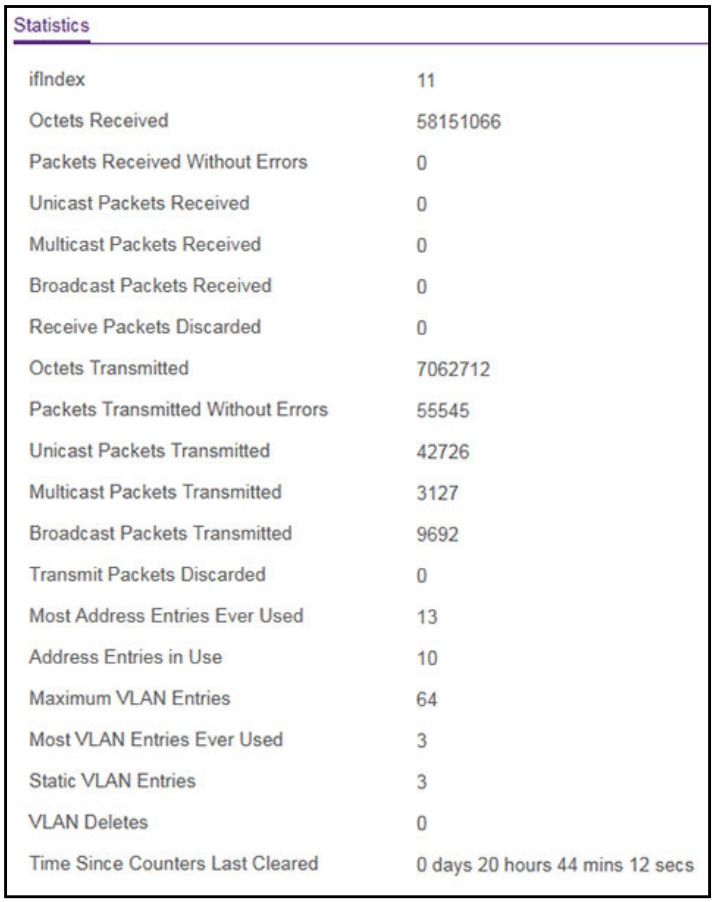
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Monitoring > Ports > Switch Statistics**.



6. Click the **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 displayed on the page.

Table 58. 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.

Table 58. Switch statistics (continued)

Field	Description
Broadcast Packets Received	The total number of 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 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 view a summary of per-port traffic statistics on the switch.

To view port statistics:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

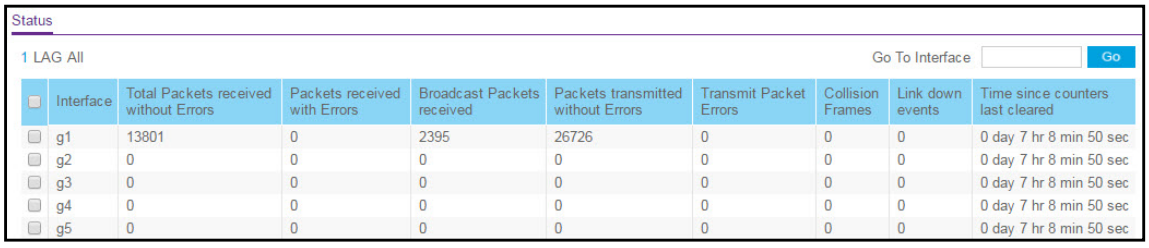
   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Ports > Port Statistics**.



6. Select whether to display physical interfaces, link aggregation groups (LAGs), or both by clicking one of the following links above the table heading:
   - **1** (or the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only link aggregation groups are displayed.
   - **All**. Both physical interfaces and link aggregation groups are displayed.
7. Select one or more interfaces by taking one of the following actions:
   - To view a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To view multiple interfaces, select the check box associated with each interface.

The following table describes the per-port statistics displayed on the page.

Table 59. Port statistics

Field	Description
Interface	The interface or LAG.
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 without errors that were transmitted by the port.
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.
Link Down Events	The total number of link down events on a physical port.
Time Since Counters Last Cleared	The elapsed time in days, hours, minutes, and seconds since the statistics for the 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 Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Ports > Port Statistics**.

   The Port Statistics page displays.

6. Select the check box in the heading of the table.
7. Click the **Clear** button.

   All counters are reset to 0.

Reset Counters for One or More Specific Interfaces

To reset the counters for one or more specific interfaces:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Monitoring > Ports > Port Statistics**.

   The Port Statistics page displays.
6. Select whether to display physical interfaces, LAGs, or both by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **All**. Both physical interfaces and LAGs are displayed.
7. Select one or more interfaces by taking one of the following actions:
   - To reset a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To reset multiple interfaces, select the check box associated with each interface.
8. Click the **Clear** button.

   The counters for the interface are reset to 0.

View and Manage Detailed Port Statistics

You can view a variety of per-port traffic statistics.

To view and manage detailed port statistics:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

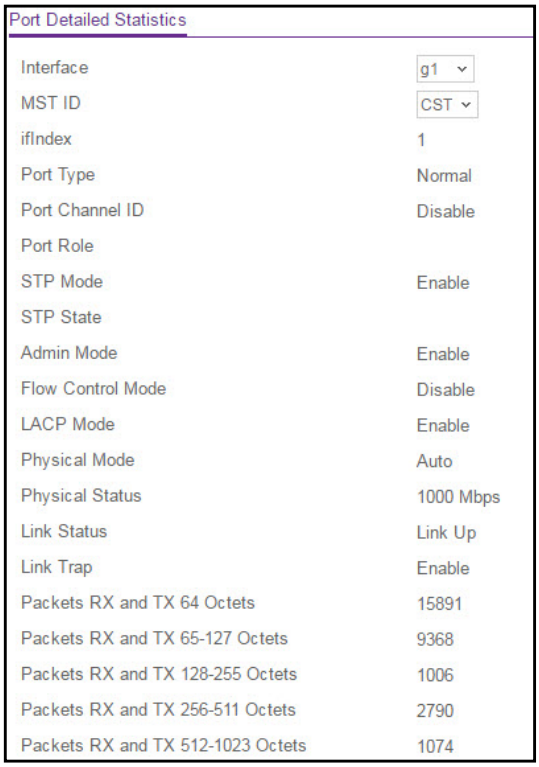
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Monitoring > Ports > Port Detailed Statistics**.



The previous figure does not show all fields on the Port Detailed Statistics page.

6. From the **Interface** menu, select the interface for which you want to view the statistics.
7. From the **MST ID** menu, select the MST ID associated with the interface (if available).
8. To refresh the page with the latest information about the switch, click the **Update** button.
9. To clear all the counters, click the **Clear** button. This resets all statistics for the port to the default values.

The following table describes the detailed port information that displays for a particular port.

Table 60. Detailed port statistics

Field	Description
ifIndex	The interface or LAG.
Port Type	For normal ports this field displays Normal. Otherwise, the options are as follows: • **Mirrored**. The port is a participating in port mirroring as a mirrored port. • **Probe**. The port is a participating in port mirroring as the probe port. • **Port Channel**. The port is a member of a LAG.
Port Channel ID	If the port is a member of a port channel (LAG), the port channel's interface ID and name are shown. Otherwise, Disable is shown.
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 that is associated with the port or port channel. The options are as follows: • **Enable**. Spanning tree is enabled for the port. • **Disable**. Spanning tree is disabled for the 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: • 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 does not apply to LAGs.
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.

Table 60. Detailed port statistics (continued)

Field	Description
Physical Status	Indicates the port speed and duplex mode for physical interfaces.
Link Status	Indicates whether the link is up or down.
Link Trap	Indicates whether or not 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).
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).
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 you need greater precision, 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).

Table 60. Detailed port statistics (continued)

Field	Description
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.
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.
Total Received Packets Not Forwarded	The number of valid frames received that were discarded (that is, filtered) by the forwarding process.

Table 60. Detailed port statistics (continued)

Field	Description
802.3x Pause Frames Received	The number of MAC control frames received on the interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
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 yo need greater precision, 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).
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 successfully by the port.
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.

Table 60. Detailed port statistics (continued)

Field	Description
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	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Excessive Collision Frames	The number of frames for which transmission on a particular interface fails due to excessive collisions.
Dropped Transmit Frames	The number of transmit frames discarded at the selected port.
STP BPDUs Received	The number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	The number of STP BPDUs transmitted from the selected port.
RSTP BPDUs Received	The number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	The number of RSTP BPDUs transmitted from the selected port.
MSTP BPDUs Received	The number of MSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	The number of MSTP BPDUs transmitted from the selected port.
802.3x Pause Frames Transmitted	The number of MAC control frames transmitted on the interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
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 the port were last cleared.

View or Clear EAP and EAPoL Statistics

You can view information about Extensible Authentication Protocol (EAP) and EAP over LAN (EAPoL) packets that are received on physical ports.

To view or clear EAP and EAPoL statistics:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

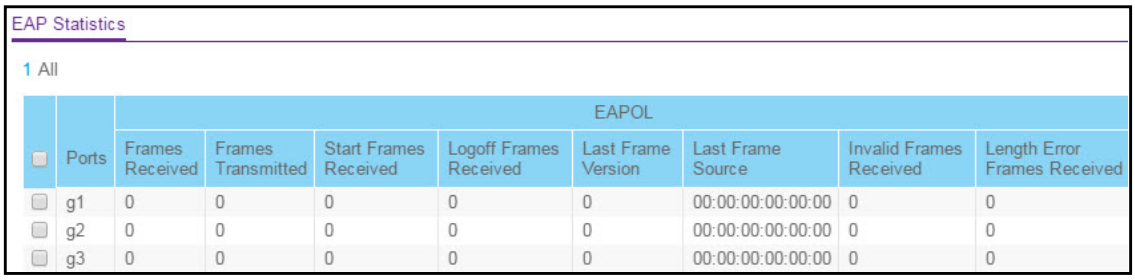
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Monitoring > Ports > EAP Statistics**.



   The previous figure does not show all fields on the EAP Statistics page.
6. To refresh the page with the latest information about the switch, click the **Update** button.
7. To clear the counters, which resets the EAP and EAPoL statistics to default values, take one of the following actions:
   - To clear the counters for a specific port, select the check box associated with the port, and click the **Clear** button.
   - To clear the counters for multiple ports, select the check boxes associated with the ports, and click the **Clear** button.
   - To clear all counters for all ports, select the check box in the row heading, and click the **Clear** button.

The following table describes the EAP statistics displayed on the page.

Table 61. EAP statistics

Field	Description
Port	The port number.
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.
EAPOL Start Frames Received	The number of EAPoL start frames that were received by this authenticator.
EAPOL Logoff Frames Received	The number of EAPoL logoff frames that were received by this authenticator.
EAPOL Last Frame Version	The protocol version number carried in the most recently received EAPoL frame.
EAPOL Last Frame Source	The source MAC address carried in the most recently received EAPoL frame.
EAPOL Invalid Frames Received	The number of EAPoL frames that were received by this authenticator in which the frame type is not recognized.
EAPOL Length Error Frames Received	The number of EAPoL frames that were received by this authenticator in which the frame type is not recognized.
EAP Response/ID Frames Received	The number of EAP response/identity frames that were received by this authenticator.
EAP Response Frames Received	The number of valid EAP response frames (other than resp/ID frames) that were received by this authenticator.
EAP Request/ID Frames Transmitted	The number of EAP request/identity frames that were transmitted by this authenticator.
EAP Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that were transmitted by this authenticator.

Perform a Cable Test

You can test and view information about the cables that are connected to switch ports.

To perform a cable test:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

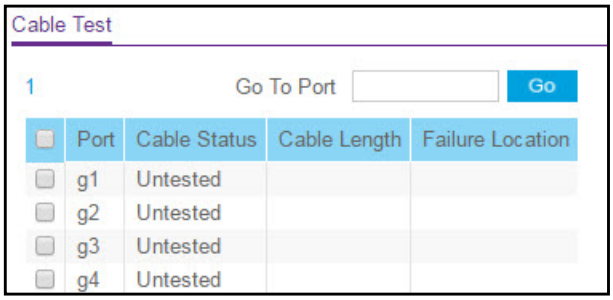
The login window opens.

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**.



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 displayed on the page.

Table 62. Cable Test information

Field	Description
Cable Status	Indicates the cable status: • **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.

Table 62. Cable Test information (continued)

Field	Description
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

The memory log stores messages in memory based upon the settings for message component and severity. You can set the administrative status and behavior of logs in the system buffer. These log messages are cleared when the switch reboots.

To configure the memory log settings:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Logs > Memory Log**.

   The Memory Log page displays.

6. Select one of the following Admin Status radio buttons:
   - **Enable**. Enable system logging. This is the default setting.
   - **Disable**. Prevent the system from logging messages.
7. From the **Behavior** menu, specify the behavior of the log when it is full.
   - **Wrap**. When the buffer is full, the oldest log messages are deleted as the system logs new messages.
   - **Stop on Ful**l. When the buffer is full, the system stops logging new messages and preserves all existing log messages.
8. From the **Severity Filter** menu, select one of the following severity levels:
   - **Emergency (0)**. System is unusable.
   - **Alert (1)**. Action must be taken immediately.
   - **Critical (2)**. Critical conditions.
   - **Error (3)**. Error conditions.
   - **Warning (4)**. Warning conditions.
   - **Notice (5)**. Normal but significant conditions.
   - **Informational (6)**. Informational messages.
   - **Debug (7)**. Debug-level messages.

   Note: A log records messages equal to or above a configured severity threshold.

9. Click the **Apply** button.

   Your settings are saved.

   The Memory Log table displays on the Memory Log page.

   The Total number of Messages field displays the number of messages the system logged in memory. Only the 200 most recent entries are displayed on the page.

   The rest of the page displays the Memory Log messages. The format of the log message is the same for messages that are displayed for the message log, persistent log, or console log. Messages logged to a collector or relay through syslog support the same format as well.

   The following example shows the standard format for a log message:

   ```
   *Jan 01 2018 00:00:18: AAA-5-CONNECT: New http connection for user
   admin, source 192.168.1.111 ACCEPTED
   ```

   The message was generated by component AAA on January 1, 2018 at 00:00:18 a.m. with severity 5 (Notice). The message indicates that the administrator logged on to the HTTP management interface from a host with IP address 192.168.1.111.

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.

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 the flash log settings:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Monitoring > Logs > FLASH Log**.

   The FLASH Log Configuration page displays.
6. Select one of the following Admin Status radio buttons:
   - **Enable**. A log that is enabled logs messages.
   - **Disable**. A log that is disabled does not log messages.
7. From the **Severity Filter** menu, select the logging level for messages that must be sent to the logging host.

   Log messages with the selected severity level and all log messages of greater severity are sent to the host. For example, if you select **Error**, the logged messages include Error, Critical, Alert, and Emergency. The default severity level is Alert (1). The severity can be one of the following levels:

   - **Emergency** (0). The highest warning level. If the device is down, or not functioning properly, an emergency log message is saved to the device.

- **Alert** (1). The second-highest warning level. An alert log message is saved if a serious device malfunction occurs, such as all device features being down. Action must be taken immediately.
- **Critical** (2). The third-highest warning level. A critical log message is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
- **Error** (3). A device error occurred, such as a port being offline.
- **Warning** (4). The lowest level of a device warning.
- **Notice** (5). Normal but significant conditions. Provides the network administrators with device information.
- **Informational** (6). Provides device information.
- **Debug** (7). Provides detailed information about the device.

8. From the **Logs to be Displayed** menu, select one of the following options:
   - **Current Logs**. The log messages for the current switch session are displayed. This is the default setting.
   - **Previous Logs**. The previous log messages are displayed, that is, the log messages that are still in the flash memory from before the switch was rebooted.
9. Click the **Apply** button.

   Your settings are saved.

   The Total Number of Messages field shows is the total number of persistent log messages that are stored on the switch. The maximum number of persistent log messages displayed on the switch is 64.

   ```
   *Jan 01 2018 00:00:18: AAA-5-CONNECT: New http connection for user
   admin, source 192.168.1.111 ACCEPTED
   ```

   The message was generated by component AAA on January 1, 2018 at 00:00:18 a.m. with severity 5 (Notice). The message indicates that the administrator logged on to the HTTP management interface from a host with IP address 192.168.1.111.

Manage the Server Log

You can let the switch send log messages to remote logging hosts. A remote log server is the same as a remote syslog host.

You must enable the server log on the switch and specify one or more remote syslog hosts.

Enable the Server Log and Add a Remote Syslog Host

To enable the server log and add a remote syslog host:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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. In the Server Log Configuration section, select one of the following Admin Status radio buttons:
   - **Enable**. Send log messages to all configured hosts (syslog collectors or relays) using the values configured for each host.
   - **Disable**. Stop logging to all syslog hosts. **Disable** means no messages are sent to any collector or relay.
7. Click the **Apply** button.

   Your settings are saved.
8. In the Server Configuration section, specify the following settings:
   - **IP Address Type**. Specify the IP address type of the host, which can be **IPv4** or **DNS**.
   - **Host Address**. Specify the IP address or host name of the syslog host.
   - **Port**. Specify the port on the host to which syslog messages must be sent. The default port number is 514.
   - **Severity Filter**. Use the menu to select the severity of the logs that must be sent to the logging host. Logs with the selected severity level and all logs of greater severity are sent to the host. For example, if you select **Error**, the logged messages include Error, Critical, Alert, and Emergency. The default severity level is Alert (1). The severity can be one of the following levels:
     - **Emergency** (0). The highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
     - **Alert** (1). The second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
     - **Critical** (2). The third-highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
     - **Error** (3). A device error occurred, such as a port being offline.

- **Warning** (4). The lowest level of a device warning.
- **Notice** (5). Provides the network administrators with device information.
- **Informational** (6). Provides device information.
- **Debug** (7). Provides detailed information about the log.

9. Click the **Add** button.

   The remote syslog host is added.

   The Status field in the Server Configuration table shows whether the remote logging host is currently active.

Modify the Settings for a Remote Syslog Host

To modify the settings for a remote syslog host:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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.

   Your settings are saved.

Delete the Settings for a Remote Syslog Host

To delete the settings for a remote syslog host:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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 or Clear the Trap Logs and the Counters

You can view information about the SNMP traps generated on the switch.

You can also display information about the traps that were sent.

To view or clear the trap logs and counters:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

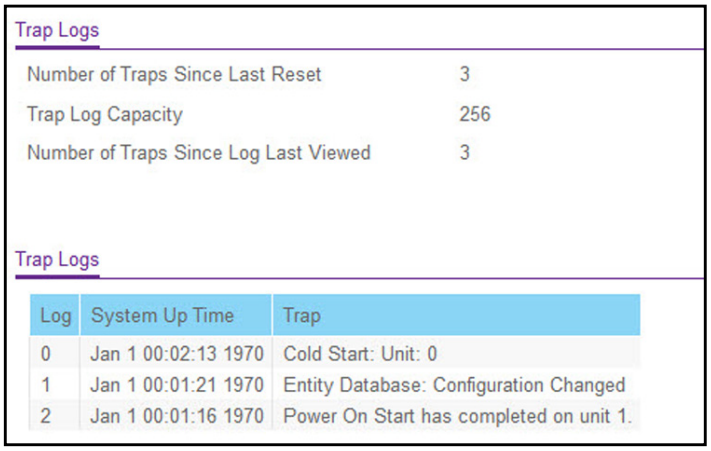
The login window opens.

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**.



6. To refresh the page with the latest information about the switch, click the **Update** button.
7. To clear the messages from the trap logs in the memory and clear the counters, click the **Clear** button.

The following table describes the Trap Log information that is displayed on the page.

Table 63. 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.
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 lets you select the network traffic of specific switch ports for analysis by a network analyzer. You can select many switch ports as source ports but a single switch port only as the destination port. You can configure how traffic is mirrored on a source port by selecting packets that are received, transmitted, or both.

A packet that is copied to the destination port is in the same format as the original packet on the wire. This means that if the mirror is copying a received packet, the copied packet is VLAN-tagged or untagged as it was received on the source port. If the mirror is copying a transmitted packet, the copied packet is VLAN-tagged or untagged as it is being transmitted on the source port.

To globally enable port mirroring, specify the destination port, and specify one or more source ports:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

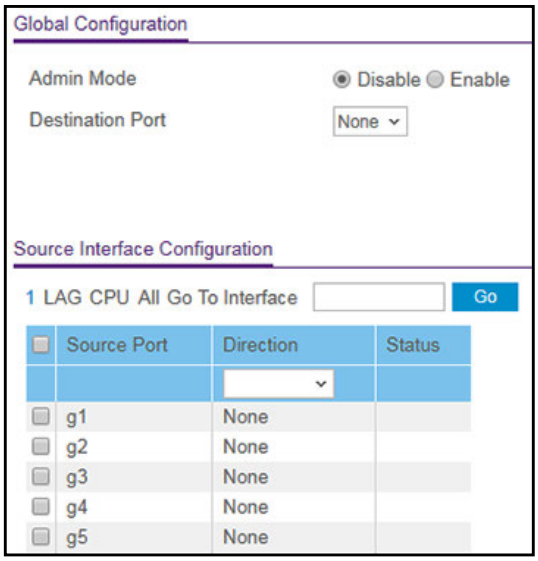
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Monitoring > Mirroring > Port Mirroring**.



6. Select an Admin Mode radio button:
   - **Disable**. Port mirroring is disabled. This is the default setting.
   - **Enabled**. Port mirroring is enabled.
7. From the **Destination Port** menu, select the physical destination port to which port traffic must be copied.

   You can configure one destination port only. The port functions as a probe port and receives traffic from all configured source ports. If no port is configured, None is displayed. The default is None.
8. Click the **Apply** button.

   Your settings are saved.

   In the Source Interface Configuration section, perform the following steps.
9. Select whether to display physical interfaces, LAGs, the CPU, or al by clicking one of the following links above the table heading:
   - **1** (the unit ID of the switch). Only physical interfaces are displayed. This is the default setting.
   - **LAG**. Only LAGs are displayed.
   - **CPU**. Only the CPU is displayed.
   - **All**. The physical interfaces, LAGs, and CPU are displayed.
10. Select one or more interfaces by taking one of the following actions:
    - To select a single interface, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
    - To select multiple interfaces, select the check box associated with each interface.

    Traffic from the selected ports will be sent to the destination port.

11. From the **Direction** menu, specify the direction of the traffic that must be mirrored from the selected source ports:
    - **None**. No traffic direction is selected. This is the default setting.
    - **Tx and Rx**. Monitors both transmitted and received packets.
    - **Rx**. Monitors received (ingress) packets only.
    - **Tx**. Monitors transmitted (egress) packets only.
12. Click the **Apply** button.

    Your settings are saved.

    The Status field indicates the interface status.

7

Maintenance

This chapter contains the following sections:

- Reboot the Switch
- Reset the Switch to Its Factory Default Settings
- Export a File From the Switch
- Download a File to the Switch or Update the Firmware
- Manage Software Images
- Perform Diagnostics and Troubleshooting

Reboot the Switch

You can reboot the switch from the local browser interface.

To reboot the switch:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Maintenance > Reset > Device Reboot**.

   The Device Reboot page displays.
6. Select the check box.
7. Click the **Apply** button.

   A confirmation pop-up window opens.
8. Click the **Yes** button to confirm.

   The switch reboots.

Reset the Switch to Its Factory Default Settings

You can reset the system configuration to the factory default values. All changes that you made are lost. If the IP address changes, your web session might disconnect.

Note: If you reset the switch to the default configuration, the IP address is reset to 192.168.0.239, and the DHCP client is enabled. If you lose network connectivity after you reset the switch to the factory defaults, see Discover or Change the Switch IP Address on page 12.

To reset the switch to the factory default settings:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Maintenance > Reset > Factory Default**.

   The Default Settings page displays.
6. Select the check box.
7. Click the **Apply** button.

   A confirmation pop-up window opens.
8. Click the **Yes** button to confirm.

   All configuration settings are reset to their factory default values. All changes that you made are lost, even if you saved the configuration.

Export a File From the Switch

You can export configuration (ASCII) or log (ASCII log) files from the switch to a file server by using TFTP or to a computer by using HTTP.

The following sections describe how you can export a file from the switch:

- Use TFTP to Export a File From the Switch to a TFTP Server on page 316
- Use HTTP to Export a File from the Switch to a Computer on page 318

Use TFTP to Export a File From the Switch to a TFTP Server

You can upload (export) configuration (ASCII or log ASCII) files from the switch to a TFTP server on the network.

To export a file from the switch to a TFTP server:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Export > TFTP File Export**.

6. From the **File Type** menu, select the type of file:
   - **Text Configuration**. A text-based configuration file enables you to edit a configured text file (`startup-config`) offline as needed. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name or IP address), and download it to that device. This is the default setting.
   - **Trap Log**. The trap log with the switch trap records.
   - **Buffered Log**. The switch buffered (in-memory) log.
   - **Tech Support**. The tech support file is a text-base file that contains a variety of hardware, software, and configuration information that can assist in device and network troubleshooting.
   - **Crash Logs**. The switch crash logs, if any are available.
7. From the **Server Address Type** menu, select the format for the **Server Address** field:
   - **IPv4**. Indicates that the TFTP server address is an IP address in dotted-decimal format. This is the default setting.
   - **DNS**. Indicates that the TFTP server address is a host name.
8. In the **Server Address** field, enter the IP address of the server in accordance with the format indicated by the server address type.

   The default is the IPv4 address 0.0.0.0.
9. In the **Transfer File Path** field, specify the path on the TFTP server where you want to save the file.

   You can enter up to 32 characters. Include the backslash at the end of the path. A path name with a space is not accepted. Leave this field blank to save the file to the root TFTP directory.
10. In the **Transfer File Name** field, specify a destination file name for the file to be uploaded.

    You can enter up to 32 characters. The transfer fails if you do not specify a file name.
11. Select the **Start File Transfer** check box.
12. Click the **Apply** button.

    The file transfer begins.

    The page displays information about the file transfer progress. The page refreshes automatically when the file transfer completes.

Use HTTP to Export a File from the Switch to a Computer

You can upload (export) files of various types from the switch to a computer through an HTTP session by using your web browser.

To export a file from the switch to a computer by using HTTP:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Export > HTTP File Export**.

   The HTTP File Export page displays.

6. From the **File Type** menu, select the type of file:
   - **Text Configuration**. A text-based configuration file enables you to edit a configured text file (`startup-config`) offline as needed. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name or IP address), and download it to that device.
   - **Tech Support**. The tech support file is a text-base file that contains a variety of hardware, software, and configuration information that can assist in device and network troubleshooting.
   - **Crash Logs**. The switch crash logs, if any are available.
7. Click the **Apply** button.

   The file transfer begins.

   The page displays information about the file transfer progress. The page refreshes automatically when the file transfer completes.

Download a File to the Switch or Update the Firmware

You can download system files from a remote system to the switch by using either TFTP or HTTP. In this context, downloading is also referred to as updating.

These procedures also include updating the switch firmware.

The following sections describe how you can download a file to the switch:

- Use TFTP to Download a File to the Switch or Update the Software Image on page 319
- Use HTTP to Download a File to the Switch or Update the Software Image on page 321

Use TFTP to Download a File to the Switch or Update the Software Image

You can download a software (firmware) image, configuration files, and SSL files from a TFTP server to the switch.

Before you download a file to the switch, the following conditions must be true:

- The file to download from the TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch contains a path to the TFTP server.

You can also download files by using HTTP. See Use HTTP to Download a File to the Switch or Update the Software Image on page 321 for additional information.

To download a file to the switch from a TFTP server:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

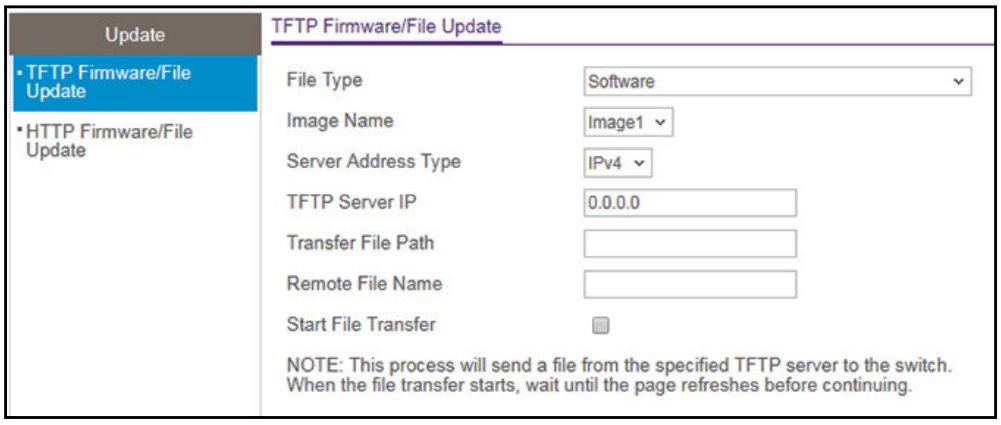
   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

The System Information page displays.

5. Select **Maintenance > Update > TFTP Firmware/File Update**.



6. From the **File Type** menu, select the type of file:
   - **Software**. The system software image, which is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy, while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the nonactive image. This is a safety feature for faults occurring during the boot upgrade process. This is the default setting.
   - **Text Configuration**. A text-based configuration file enables you to edit a configured text file (`startup-config`) offline as needed. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name or IP address), and download it to that device.
   - **SSL Trusted Root Certificate PEM File**. SSL Trusted Root Certificate File (PEM Encoded).
   - **SSL Server Certificate PEM File**. SSL Server Certificate File (PEM Encoded).
   - **SSL DH Weak Encryption Parameter PEM File**. SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).
   - **SSL DH Strong Encryption Parameter PEM File**. SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).
7. If the selection from the **File Type** menu is **Software**, the **Image Name** menu is displayed and you must select the software image that must be downloaded to the switch:
   - **image1.** Select image1 to upload image1.
   - **image2**. Select image2 to upload image2.

   Note: We recommended that you do not overwrite the active image. If you do so, the switch displays a warning that you are trying to overwrite the active image.

8. From the **Server Address Type** menu, select the format for the **TFTP Server IP** field:
   - **IPv4**. Indicates that the TFTP server address is an IP address in dotted-decimal format. This is the default setting.
   - **DNS**. Indicates that the TFTP server address is a host name.
9. In the **TFTP Server IP** field, enter the IP address of the TFTP server indicated by the server address type.

   The default is the IPv4 address 0.0.0.0.
10. In the **Transfer File Path** field, specify the path on the TFTP server where the file is located.

    Enter up to 160 characters. Include the backslash at the end of the path. A path name with a space is not accepted. Leave this field blank to save the file to the root TFTP directory.
11. In the **Remote File Name** field, specify the name of the file to download from the TFTP server.

    You can enter up to 32 characters. A file name with a space is not accepted.
12. Select the **Start File Transfer** check box to initiate the file upload.
13. Click the **Apply** button.

    The file transfer begins.

    The page displays information about the progress of the file transfer. The page refreshes automatically when the file transfer completes.

Note: After a software image file is downloaded, you might need to select the new software image file (see Change the Software Image That Loads When the Switch Starts or Reboots on page 325) and reboot the switch.

Use HTTP to Download a File to the Switch or Update the Software Image

You can download a software (firmware) image, configuration files, and SSL files from a computer to the switch by using an HTTP session over a web browser.

To download a file to the switch using HTTP:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

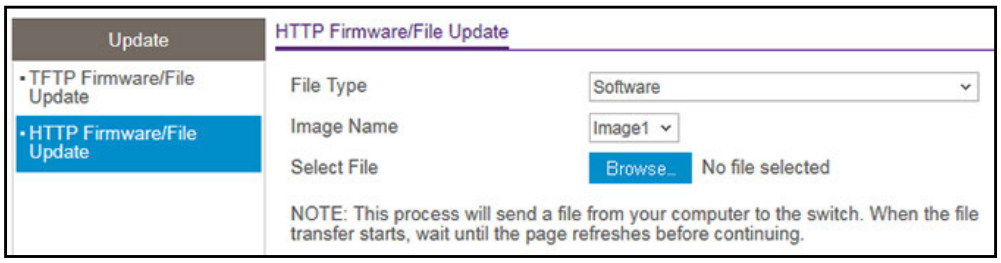
The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Update > HTTP Firmware/File Update**.



6. From the **File Type** menu, select the type of file:
   - **Software**. The system software image, which is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy, the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the nonactive image. This is a safety feature for faults occurring during the boot upgrade process. This the default setting.
   - **Text Configuration**. A text-based configuration file enables you to edit a configured text file (`startup-config`) offline as needed. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name, serial number, IP address), and download it to that device.
   - **SSL Trusted Root Certificate PEM File**. SSL Trusted Root Certificate File (PEM Encoded).
   - **SSL Server Certificate PEM File**. SSL Server Certificate File (PEM Encoded).
   - **SSL DH Weak Encryption Parameter PEM File**. SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).
   - **SSL DH Strong Encryption Parameter PEM File**. SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).
7. If the selection from the **File Type** menu is **Software**, the **Image Name** menu is displayed and you must select the software image that must be downloaded to the switch:
   - **image1.** Select image1 to upload image1.
   - **image2**. Select image2 to upload image2.

Note: We recommended that you do not overwrite the active image. If you do so, the switch displays a warning that you are trying to overwrite the active image.

8. Click the **Browse** button and locate and select the file that you want to download.

   The file name can contain up to 80 characters.

9. Click the **Apply** button.

   The file transfer begins.

   The page displays information about the progress of the file transfer. After a file transfer is started, wait until the page refreshes. When the page refreshes, the option to select a file option is no longer available, indicating that the file transfer is complete.

Note: After a software image file is downloaded, you might need to select the new software image file (see Change the Software Image That Loads When the Switch Starts or Reboots on page 325) and reboot the switch. After a text configuration file is downloaded, the switch applies the configuration automatically.

Manage Software Images

The switch maintains two versions of the switch software in permanent storage. One image is the active image, and the second image is the backup image. The active image is loaded when the switch starts or reboots. This feature reduces switch down time when you are updating the switch software.

Note: A switch that runs an older (legacy) software version might not load a configuration file that is created by a newer software version. In such a situation, the switch displays a warning.

The following sections describe how you can manage the software images:

- Copy a Software Image on page 324
- Configure Dual Image Settings on page 324

Copy a Software Image

You can copy a software image from one location (primary or backup) to another.

To copy a software image:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

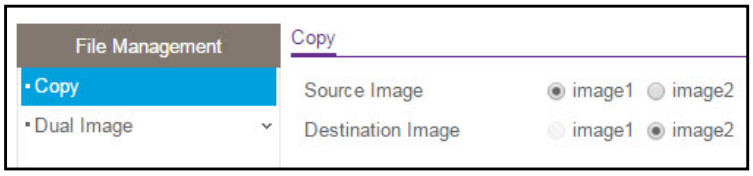
   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > File Management > Copy**.



6. Select the Source Image **image1** or **image2** radio button to specify the image to be copied.
7. Select the Destination Image **image1** or **image2** radio button to specify the destination image.
8. Click the **Apply** button.

   Your settings are saved.

Configure Dual Image Settings

The Dual Image feature allows the switch to retain two images in permanent storage. You can select which image must load when the reboots, specify an image description, or delete an image. This feature reduces switch down time when you are upgrading or downgrading the software image.

Change the Software Image That Loads When the Switch Starts or Reboots

To change the image that loads during the boot process:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

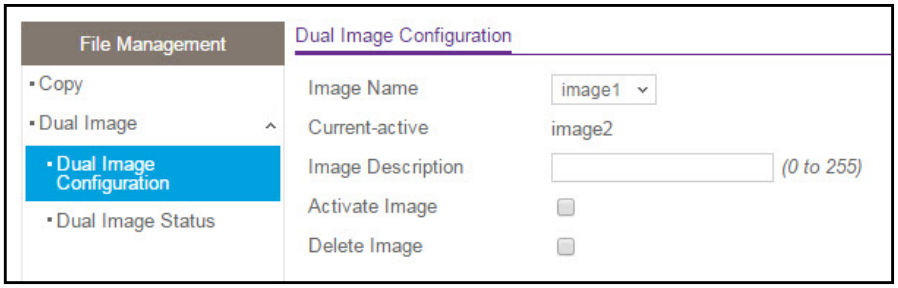
   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > File Management > Dual Image Configuration**.



6. From the **Image Name** menu, select the image that is *not* the image displayed in the Current-active field but that is the image that you want the switch to run *after* it reboots.

   The Current-active field displays the name of the active image.

7. As an option, specify a name for the selected image by entering one in the **Image Description** field.
8. Select the **Activate Image** check box.
9. Click the **Apply** button.

   Your settings are saved.

IMPORTANT:

After activating an image, you must reboot the switch. Otherwise, the switch continues running the image shown in the Current-active field until the switch reboots.

Delete a Software Image

To delete a software image:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.
4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.
5. Select **Maintenance > File Management > Dual Image Configuration**.

   The Dual Image Configuration page displays.
6. From the **Image Name** menu, select the image that is *not* the image displayed in the Current-active field.

   The Current-active field displays the name of the active image. You cannot delete the active image.
7. Select the **Delete** Image check box.
8. Click the **Apply** button.

   The image is removed.

View the Dual Image Status

You can view information about the active and backup images on the system.

To view dual image status information:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > File Management > Dual Image > Dual Image Status**.

The following table describes the information available on the page.

Table 64. Dual Image Status information

Field	Description
Image1 Ver	The version of the image1 file.
Image2 Ver	The version of the image2 file.
Current-active	The currently active image on this switch.
Next-active	The image to be used after the switch reboots.
Image1 Description	The description associated with the image1 file.
Image2 Description	The description associated with the image2 file.

Perform Diagnostics and Troubleshooting

You can use a ping or a traceroute, and you can perform a memory dump.

The following sections describe how you can troubleshoot the switch and the network:

- Ping an IPv4 Address on page 327
- Send an IPv4 Traceroute on page 329
- Enable Remote Diagnostics on page 331

Ping an IPv4 Address

You can configure the switch to send a ping request to a specified IP address. You can use this option to check whether the switch can communicate with a particular IP station. When you send a ping, 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:

```
PING x.y.z.w (x.y.z.w): size data bytes
--- x.y.z.w ping statistics ---
count packets transmitted, 0 packets received, 100% packet loss
```

If a reply to the ping is received, the following message displays:

```
PING x.y.z.w (x.y.z.w): size data bytes
size bytes from x.y.z.w: seq=0 ttl=xyz
--- x.y.z.w ping statistics ---
count packets transmitted, count packets received, x% packet loss
```

To configure the settings and ping an IPv4 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.

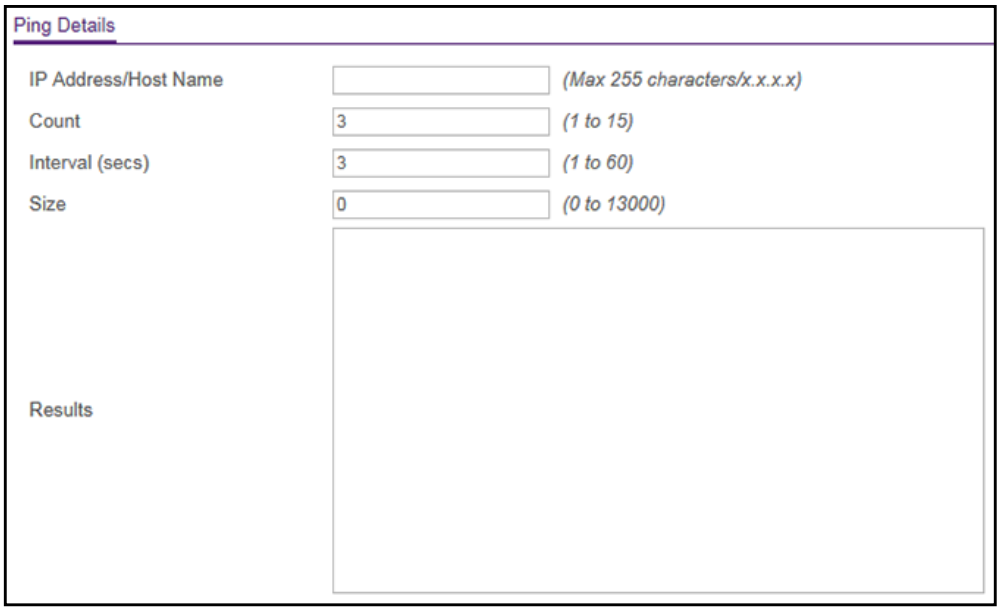
   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login 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 value is 3. The range is 1 to 15.
8. In the **Interval** field, enter the time between ping packets in seconds.

   The default value is 3 seconds. The range is 1 to 60.
9. In the **Size** field, enter the size of the ping packet. The default value is 0 bytes. The range is 0 to 13000.
10. Click the **Apply** button.

    The specified address is pinged. The results are displayed below the configurable data in the Results field.

Send an IPv4 Traceroute

You can configure the switch to send a traceroute request to a specified IP address or host name. You can use this to discover the paths that packets take to a remote destination. When you send a traceroute, the switch displays the results below the configurable data.

If a reply to the traceroute is received, the following message displays:

```
traceroute to x.y.z.w (x.y.z.w), maxTTL hops max, size byte packets
initTTL x.y.z.w (x.y.z.w) 0.000 ms * 0.000 ms
initTTL+1 x.y.z.w (x.y.z.w) 0.000 ms * 0.000 ms
initTTL+2 x.y.z.w (x.y.z.w) 0.000 ms * 0.000 ms
```

To send an IPv4 traceroute:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

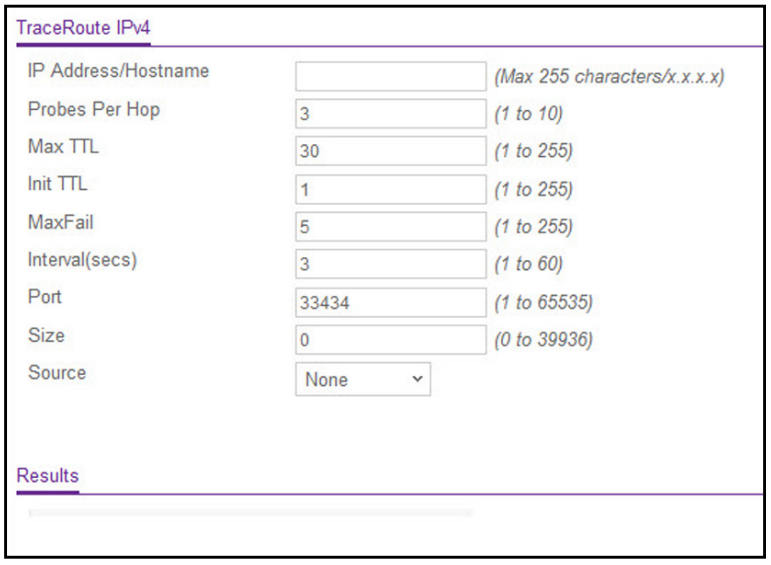
   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Troubleshooting > Traceroute IPv4**.



6. In the **IP Address/Hostname** field, enter the IP address or host name of the device for which the path must be discovered.
7. In the **Probes Per Hop** field, enter the number of probes per hop.

   The default value is 3. The range is 1 to 10.

8. In the **Max TTL** field, enter the maximum time to live (TTL) for the destination.

   The default value is 30. The range is 1 to 255.

9. In the **Init TTL** field, enter the initial TTL to be used.

   The default value is 1. The range is 1 to 255.

10. In the **MaxFail** field, enter the maximum number of failures allowed in the session.

    The default value is 5. The range is 1 to 255.

11. In the **Interval (secs)** field, enter the time between probes in seconds.

    The default value is 3. The range is 1 to 60.

12. In the **Port** field, enter the UDP destination port for the probe packets.

    The default value is 33434. The range is 1–65535.

13. In the **Size** field, enter the size of the probe packets.

    The default value is 0. The range is 32 to 32768.

14. Click the **Apply** button.

    A traceroute request is sent to the specified IP address or host name. The results are displayed below the configurable data in the Results field.

Enable Remote Diagnostics

You can enable or disable the option to access the switch remotely. When remote access is enabled, you or technical support can perform remote diagnostics services.

To enable remote diagnostics:

1. Connect your computer to the same network as the switch.

   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.

2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see Discover or Change the Switch IP Address on page 12.

   Your web browser might display a security message, which you can ignore. For more information, see Access the Local Browser Interface on page 18.

   The login window opens.

4. Enter the switch's password in the **Password** field.

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Troubleshooting > Remote Diagnostics**.

   The Remote Diagnostics page displays.

6. Select the **Enable** radio button.
7. Click the **Apply** button.

   Your settings are saved.

A

Configuration Examples

This appendix contains the following sections:

- Virtual Local Area Networks (VLANs)
- Access Control Lists (ACLs)
- Differentiated Services (DiffServ)
- 802.1X Access Control
- Multiple Spanning Tree Protocol

Virtual Local Area Networks (VLANs)

A local area network (LAN) can generally be defined as a broadcast domain. Hubs, bridges, or switches in the same physical segment or segments connect all end node devices. End nodes can communicate with each other without the need for a router. Routers connect LANs together, routing the traffic to the appropriate port.

A virtual LAN (VLAN) is a local area network with a definition that maps workstations on some basis other than geographic location (for example, by department, type of user, or primary application). To enable traffic to flow between VLANs, traffic must go through a router, just as if the VLANs were on two separate LANs.

A VLAN is a group of computers, servers, and other network resources that behave as if they were connected to a single network segment—even though they might not be. For example, all marketing personnel might be spread throughout a building. Yet if they are all assigned to a single VLAN, they can share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specified individuals, depending on how the IT manager set up the VLANs.

VLANs present a number of advantages:

- It is easy to do network segmentation. Users who communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group’s traffic is contained largely within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.
- They are easy to manage. The addition of nodes, as well as moves and other changes, can be dealt with quickly and conveniently from a management interface rather than from the wiring closet.
- They provide increased performance. VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.
- They ensure enhanced network security. VLANs create virtual boundaries that can be crossed only through a router. So standard, router-based security measures can be used to restrict access to each VLAN.

Packets received by the switch are treated in the following way:

- When an untagged packet enters a port, it is automatically tagged with the port’s default VLAN ID tag number. Each port supports a default VLAN ID setting that is user configurable (the default setting is 1). The default VLAN ID setting for each port can be changed on the Port PVID Configuration page. See Configure Port PVID Settings on page 118.
- 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 port means that packets leaving the switch from that port are untagged. Inversely, a T for a port means that packets leaving the switch from that port are tagged with the VLAN ID that is associated with the port.

The example 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 111), 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 115) 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 118), specify the PVID for ports g1 and g4 so that packets entering these ports are tagged with the port VLAN ID:
   - Port g1: PVID 10
   - Port g4: PVID 20
4. With the VLAN configuration that you set up, the following situations produce results as described:
   - If an untagged packet enters port 1, the switch tags it with VLAN ID 10. The packet can access port 2 and port 3. The outgoing packet is stripped of its tag to leave port 2 as an untagged packet. For port 3, the outgoing packet leaves as a tagged packet with VLAN ID 10.
   - If a tagged packet with VLAN ID 10 enters port 3, the packet can access port 1 and port 2. If the packet leaves port 1 or port 2, it is stripped of its tag to leave the switch as an untagged packet.

- If an untagged packet enters port 4, the switch tags it with VLAN ID 20. The packet can access port 5 and port 6. The outgoing packet is stripped of its tag to become an untagged packet as it leaves port 6. For port 5, the outgoing packet leaves as a tagged packet with VLAN ID 20.

Access Control Lists (ACLs)

ACLs ensure that only authorized users can access specific resources while blocking off any unwarranted attempts to reach network resources.

ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and provide security for the network. ACLs are normally used in firewall routers that are positioned between the internal network and an external network, such as the Internet. They can also be used on a router positioned between two parts of the network to control the traffic entering or exiting a specific part of the internal network. The added packet processing required by the ACL feature does not affect switch performance. That is, ACL processing occurs at wire speed.

Access lists are sequential collections of permit and deny conditions. This collection of conditions, known as the filtering criteria, is applied to each packet that is processed by the switch or the router. The forwarding or dropping of a packet is based on whether or not the packet matches the specified criteria.

Traffic filtering requires the following two basic steps:

1. Create an access list definition.

   The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. Additionally, you can assign traffic that matches the criteria to a particular queue or redirect the traffic to a particular port. A default *deny all* rule is the last rule of every list.

2. Apply the access list to an interface in the inbound direction.

The switch allow ACLs to be bound to physical ports and LAGs. The switch software supports MAC ACLs and IP ACLs.

MAC ACL Sample Configuration

The following example shows how to create a MAC-based ACL that permits Ethernet traffic from the Sales department on specified ports and denies all other traffic on those ports.

1. On the MAC ACL page, create an ACL with the name Sales_ACL for the Sales department of your network (see Configure a Basic MAC ACL on page 256).

   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 259.

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 263.)

   You can assign an optional sequence number to indicate the order of the access list relative to other access lists if any are already assigned to the interface and direction.

4. The MAC Binding Table displays the interface and MAC ACL binding information. (See View or Delete MAC ACL Bindings in the MAC Binding Table on page 265.)

The ACL named Sales_ACL looks for Ethernet frames with destination and source MAC addresses and MAC masks defined in the rule. Also, the frame must be tagged with VLAN ID 2, which is the Sales department VLAN. The CoS value of the frame must be 0, which is the default value for Ethernet frames. Frames that match this criteria are permitted on interfaces 6, 7, and 8 and are assigned to the hardware egress queue 0, which is the default queue. All other traffic is explicitly denied on these interfaces. To allow additional traffic to enter these ports, you must add a new Permit rule with the desired match criteria and bind the rule to interfaces 6, 7, and 8.

Standard IP ACL Sample Configuration

The following example shows how to create an IP-based ACL that prevents any IP traffic from the Finance department from being allowed on the ports that are associated with other departments. Traffic from the Finance department is identified by each packet's network IP address.

1. On the IP ACL page, create a new IP ACL with an IP ACL ID of 1. (See Configure a Basic or Extended IP ACL on page 266.)
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**. 255.255.0

For additional information about IP ACL rules, see Configure Rules for a Basic IP ACL on page 269.

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 280.)

   By default, this IP ACL is bound on the inbound direction, so it examines traffic as it enters the switch.
7. Click the **Apply** button.
8. Use the IP Binding Table page to view the interfaces and IP ACL binding information. (See View or Delete IP ACL Bindings in the IP ACL Binding Table on page 282)

The IP ACL in this example matches all packets with the source IP address and subnet mask of the Finance department's network and deny it on the Ethernet interfaces 2, 3, and 4 of the switch. The second rule permits all non-Finance traffic on the ports. The second rule is required because an explicit *deny all* rule exists as the lowest priority rule.

Differentiated Services (DiffServ)

Standard IP-based networks are designed to provide *best effort* data delivery service. *Best effort* service implies that the network delivers the data in a timely fashion, although there is no guarantee that it does. During times of congestion, packets might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. However, any degradation of service can negatively affect applications with strict timing requirements, such as voice or multimedia.

Quality of Service (QoS) can provide consistent, predictable data delivery by distinguishing between packets with strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given special treatment in a QoS-capable network. With this in mind, all elements of the network must be QoS capable. If one node cannot meet the necessary timing requirements, this creates a deficiency in the network path and the performance of the entire packet flow is compromised.

Two basic types of QoS are supported:

- **Integrated Services**. Network resources are apportioned based on request and are reserved (resource reservation) according to network management policy (RSVP, for example).
- **Differentiated Services**. Network resources are apportioned based on traffic classification and priority, giving preferential treatment to data with strict timing requirements.

The switch supports DiffServ.

The DiffServ feature contains a number of conceptual QoS building blocks that you can use to construct a differentiated service network. Use these same blocks in different ways to build other types of QoS architectures.

You must configure three key QoS building blocks for DiffServ:

- Class
- Policy
- Service (the assignment of a policy to a directional interface)

Class

You can classify incoming packets at Layers 2, 3, and 4 by inspecting the following information for a packet:

- Source/destination MAC address
- EtherType
- Class of Service (802.1p priority) value (first/only VLAN tag)
- VLAN ID range (first/only VLAN tag)
- Secondary 802.1p priority value (second/inner VLAN tag)
- Secondary VLAN ID range (second/inner VLAN tag)
- IP Service Type octet (also known as: ToS bits, Precedence value, DSCP value)
- Layer 4 protocol (TCP, UDP and so on)
- Layer 4 source/destination ports
- Source/destination IP address

From a DiffServ point of view, two types of classes exist:

- DiffServ traffic classes
- DiffServ service levels/forwarding classes

DiffServ Traffic Classes

With DiffServ, you define which traffic classes to track on an ingress interface. You can define simple BA classifiers (DSCP) and a wide variety of multifield (MF) classifiers:

- Layer 2; Layers 3, 4 (IP only)
- Protocol-based
- Address-based

You can combine these classifiers with logical AND operations to build complex MF-classifiers (by specifying a class type of *all* or *any*, respectively). That is, within a single class, multiple match criteria are grouped together as an AND expression, depending on the defined class type. Only classes of the same type can be nested; class nesting does not allow for the negation (*exclude* option) of the referenced class.

To configure DiffServ, you must define service levels, namely the forwarding classes/PHBs identified by a DSCP value, on the egress interface. You define these service levels by configuring BA classes for each.

Creating Policies

Use DiffServ policies to associate a collection of classes that you configure with one or more QoS policy statements. The result of this association is referred to as a policy.

From a DiffServ perspective, two types of policies exist:

- **Traffic Conditioning Policy**. A policy applied to a DiffServ traffic class
- **Service Provisioning Policy**. A policy applied to a DiffServ service level

You must manually configure the various statements and rules used in the traffic conditioning and service provisioning policies to achieve the desired Traffic Conditioning Specification (TCS) and the Service Level Specification (SLS) operation, respectively.

Traffic Conditioning Policy

Traffic conditioning pertains to actions performed on incoming traffic. Several distinct QoS actions are associated with traffic conditioning:

- **Dropping**. Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot coexist on the same interface.
- **Marking IP DSCP or IP Precedence**. Marking/re-marking the DiffServ code point in a packet with the DSCP value representing the service level associated with a particular DiffServ traffic class. Alternatively, the IP precedence value of the packet can be marked/re-marked.
- **Marking CoS (802.1p)**. Sets the 3-bit priority field in the first/only 802.1p header to a specified value when packets are transmitted for the traffic class. An 802.1p header is inserted if it does not already exist. This is useful for assigning a Layer 2 priority level based on a DiffServ forwarding class (such as the DSCP or IP precedence value)

definition to convey some QoS characteristics to downstream switches that do not routinely look at the DSCP value in the IP header.

- **Policing**. A method of constraining incoming traffic associated with a particular class so that it conforms to the terms of the TCS. Out-of-profile packets that are either in excess of the conformance specification or are nonconformant are dropped.
- **Counting**. Updating octet and packet statistics to keep track of data handling along traffic paths within DiffServ. In this DiffServ feature, counters are not explicitly configured by the user, but are designed into the system based on the DiffServ policy being created. For more information, see Monitor the Switch and the Ports on page 287.
- **Assigning QoS Queue**. Directs a traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.
- **Redirecting**. Forces a classified traffic stream to a specified egress port (physical or LAG). This can occur in addition to any marking or policing action. It can also be specified along with a QoS queue assignment.

DiffServ Example Configuration

To create a DiffServ class and policy and attach them to a switch interface, follow these steps:

1. On the QoS Class Configuration page, create a new class with the following settings:
   - **Class Name**. Class1
   - **Class Type**. All

   For more information, see Configure a DiffServ Class on page 184.
2. Click the **Class1** hyperlink to view the DiffServ Class Configuration page for this class.
3. Configure the following settings for Class1:
   - **Protocol Type**. UDP
   - **Source IP Address**. 192.12.1.0.
   - **Source Mask**. 255.255.255.0.
   - **Source L4 Port**. Other, and enter 4567 as the source port value.
   - **Destination IP Address**. 192.12.2.0.
   - **Destination Mask**. 255.255.255.0.
   - **Destination L4 Port**. Other, and enter 4568 as the destination port value.

   For more information, see Configure a DiffServ Class on page 184.
4. Click the **Apply** button.
5. On the Policy Configuration page, create a new policy with the following settings:
   - **Policy Selector**. Policy1
   - **Member Class**. Class1

   For more information, see Configure a DiffServ Policy on page 190.

6. Click the **Add** button.

   The policy is added.

7. Click the **Policy1** hyperlink to view the Policy Class Configuration page for this policy.
8. Configure the Policy attributes as follows:
   - **Assign Queue**. 3
   - **Policy Attribute**. Simple Policy
   - **Color Mode**. Color Blind
   - **Committed Rate**. 1000000 Kbps
   - **Confirm Action**. Send
   - **Violate Action**. Drop

   For more information, see Configure a DiffServ Policy on page 190.

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 195.)

All UDP packet flows destined to the 192.12.2.0 network with an IP source address from the 192.12.1.0 network that include a Layer 4 Source port of 4567 and Destination port of 4568 from this switch on ports 7 and 8 are assigned to hardware queue 3.

On this network, traffic from streaming applications uses UDP port 4567 as the source and 4568 as the destination. This real-time traffic is time sensitive, so it is assigned to a high-priority hardware queue. By default, data traffic uses hardware queue 0, which is designated as a best-effort queue.

Also the *confirmed action* on this flow is to send the packets with a committed rate of 1000000 Kbps. Packets that violate the committed rate and burst size are dropped.

802.1X Access Control

Local area networks (LANs) are often deployed in environments that permit unauthorized devices to be physically attached to the LAN infrastructure, or permit unauthorized users to attempt to access the LAN through equipment already attached. In such environments you might want to restrict access to the services offered by the LAN to those users and devices that are permitted to use those services.

Port-based network access control makes use of the physical characteristics of LAN infrastructures to provide a means of authenticating and authorizing devices attached to a LAN port with point-to-point connection characteristics. If the authentication and authorization process fails, access control prevents access to that port. In this context, a port is a single point of attachment to the LAN, such as a port of a MAC bridge and an association between stations or access points in IEEE 802.11 wireless LANs.

The IEEE 802.11 standard describes an architectural framework within which authentication and consequent actions take place. It also establishes the requirements for a protocol

between the authenticator (the system that passes an authentication request to the authentication server) and the supplicant (the system that requests authentication), as well as between the authenticator and the authentication server.

The switch supports a guest VLAN, which allows unauthenticated users limited access to the network resources.

Note: You can use QoS features to provide rate limiting on the guest VLAN to limit the network resources that the guest VLAN provides.

Another 802.1X feature is the ability to configure a port to enable or disable EAPoL packet forwarding support. You can disable or enable the forwarding of EAPoL when 802.1X is disabled on the device.

The ports of an 802.1X authenticator switch provide the means by which it can offer services to other systems reachable through the LAN. Port-based network access control allows the operation of a switch’s ports to be controlled to ensure that access to its services is permitted only by systems that are authorized to do so.

Port access control provides a means of preventing unauthorized access by supplicants to the services offered by a system. Control over the access to a switch and the LAN to which it is connected can be desirable when you restrict access to publicly accessible bridge ports or to restrict access to departmental LANs.

Access control is achieved by enforcing authentication of supplicants that are attached to an authenticator's controlled ports. The result of the authentication process determines whether the supplicant is authorized to access services on that controlled port.

A port access entity (PAE) is able to adopt one of two distinct roles within an access control interaction:

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.

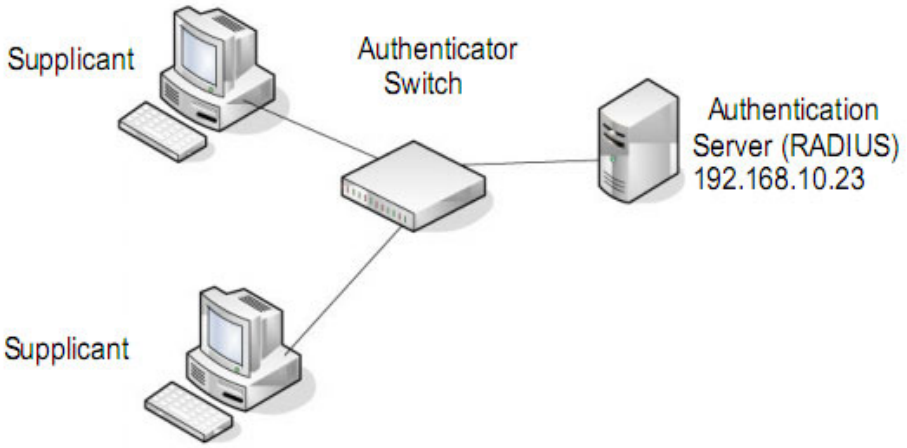


Figure 1. 802.1X authentication roles

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 (1/0/5–1/0/8). These ports are available to visitors and must be authenticated before access is granted to the network. The authentication is handled by an external RADIUS server. When the visitor is successfully authenticated, traffic is automatically assigned to the guest VLAN. This example assumes that a VLAN was configured with a VLAN ID of 150 and VLAN name of Guest.

1. On the Port Authentication page, select ports **1/0/5**, **1/0/6**, **1/0/7**, and **1/0/8**.
2. From the **Port Control** menu, select **Unauthorized**.

   The selection from the **Port Control** menu for all other ports on which authentication is not needed must be **Authorized**. When the selection from the **Port Control** menu is **Authorized**, the port is unconditionally put in a force-authorized state and does not require any authentication. When the selection from the **Port Control** menu is **Auto**, the authenticator PAE sets the controlled port mode.
3. In the **Guest VLAN** field for ports 1/0/5–1/0/8, enter **150** to assign these ports to the guest VLAN.

   You can configure additional settings to control access to the network through the ports. See Configure a Port Security Interface on page 247 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 246.)

   This example uses the default values for the port authentication settings, but you can configure several additional settings. For example, the **EAPOL Flood Mode** field allows you to enable the forwarding of EAPoL frames when 802.1X is disabled on the device.
6. On the RADIUS Server Configuration page, configure a RADIUS server with the following settings:

- **Server Address**. 192.168.10.23
- **Secret Configured**. Yes
- **Secret**. secret123
- **Active**. Primary

For more information, see Manage the RADIUS Settings on page 200.

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 212.)

This example enables 802.1X-based port security on the switch and prompts the hosts connected on ports g5-g8 for an 802.1X-based authentication. The switch passes the authentication information to the configured RADIUS server.

Multiple Spanning Tree Protocol

Spanning Tree Protocol (STP) runs on bridged networks to help eliminate loops. If a bridge loop occurs, the network can become flooded with traffic. IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) supports multiple instances of spanning tree to efficiently channel VLAN traffic over different interfaces. Each instance of the spanning tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree, with slight modifications in the working but not the end effect (chief among the effects is the rapid transitioning of the port to the forwarding state).

The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full-duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to the Forwarding state and the suppression of Topology Change Notification. These features are represented by the parameters pointtopoint and edgeport. MSTP is compatible to both RSTP and STP. It behaves in a way that is appropriate for STP and RSTP bridges.

An MSTP bridge can be configured to behave entirely as a RSTP bridge or an STP bridge. So, an IEEE 802.1s bridge inherently also supports IEEE 802.1w and IEEE 802.1D.

The MSTP algorithm and protocol provide simple and full connectivity for frames assigned to any VLAN throughout a bridged LAN comprising arbitrarily interconnected networking devices, each operating MSTP, STP, or RSTP. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) regions composed of LANs and or MSTP bridges. These regions and the other bridges and LANs are connected into a single Common Spanning Tree (CST). (IEEE DRAFT P802.1s/D13)

MSTP connects all bridges and LANs with a single Common and Internal Spanning Tree (CIST). The CIST supports the automatic determination of each MST region, choosing its maximum possible extent. The connectivity calculated for the CIST provides the CST for interconnecting these regions, and an Internal Spanning Tree (IST) within each region.

MSTP ensures that frames with a VLAN ID are assigned to one and only one of the MSTIs or the IST within the region, that the assignment is consistent among all the networking devices in the region, and that the stable connectivity of each MSTI and IST at the boundary of the region matches that of the CST. The stable active topology of the bridged LAN with respect to frames consistently classified as belonging to any VLAN thus simply and fully connects all LANs and networking devices throughout the network, though frames belonging to different VLANs can take different paths within any region, per IEEE DRAFT P802.1s/D13.

All bridges, whether they use STP, RSTP, or MSTP, send information in configuration messages through Bridge Protocol Data Units (BPDUs) to assign port roles that determine each port's participation in a fully and simply connected active topology based on one or more spanning trees. The information communicated is known as the spanning tree priority vector. The BPDU structure for each of these different protocols is different. An MSTP bridge transmits the appropriate BPDU depending on the received type of BPDU from a particular port.

An MST region comprises of one or more MSTP bridges with the same MST configuration identifier, using the same MSTIs, and without any bridges attached that cannot receive and transmit MSTP BPDUs. The MST configuration identifier includes the following components:

1. Configuration identifier format selector
2. Configuration name
3. Configuration revision level
4. Configuration digest: 16-byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID to MSTID mapping)

Because multiple instances of spanning tree exist, an MSTP state is maintained on a per-port, per-instance basis (or on a per-port, per-VLAN basis, as any VLAN can be in one and only one MSTI or CIST). For example, port A can be forwarding for instance 1 while discarding for instance 2. The port states changed since IEEE 802.1D specification.

To support multiple spanning trees, configure an MSTP bridge with an unambiguous assignment of VLAN IDs (VIDs) to spanning trees. For such a configuration, ensure the following:

1. The allocation of VIDs to FIDs is unambiguous.
2. Each FID that is supported by the bridge is allocated to exactly one spanning tree instance.

The combination of VID to FID and then FID to MSTI allocation defines a mapping of VIDs to spanning tree instances, represented by the MST Configuration Table.

With this allocation we ensure that every VLAN is assigned to one and only one MSTI. The CIST is also an instance of spanning tree with an MSTID of 0.

VIDs might be not be allocated to an instance, but every VLAN must be allocated to one of the other instances of spanning tree.

The portion of the active topology of the network that connects any two bridges in the same MST region traverses only MST bridges and LANs in that region, and never bridges of any kind outside the region. In other words, connectivity within the region is independent of external connectivity.

MSTP Example Configuration

This example shows how to create an MSTP instance from the switch. The example network includes three different switches that serve different locations in the network. In this example, ports 1/0/1–1/0/5 are connected to host stations, so those links are not subject to network loops. Ports 1/0/6–1/0/8 are connected across switches 1, 2, and 3.

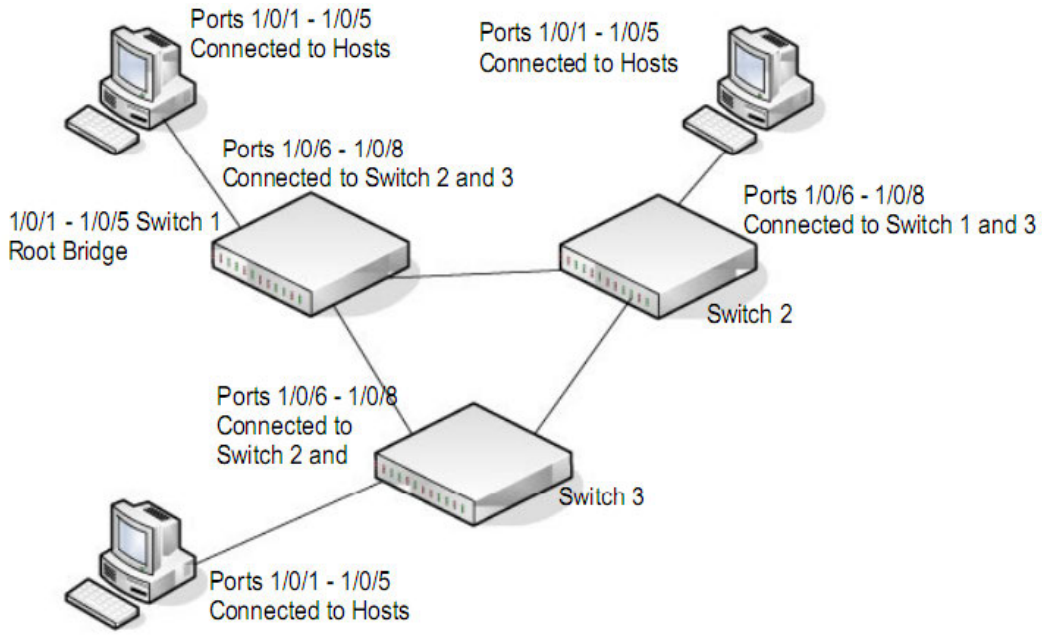


Figure 2. MSTP sample configuration

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 112).
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 112).
3. On the STP Configuration page, enable the Spanning Tree State option (see Configure the STP Settings and View the STP Status on page 133).

   Use the default values for the rest of the STP configuration settings. By default, the STP operation mode is MSTP and the configuration name is the switch MAC address.
4. On the CST Configuration page, set the bridge priority value for each of the three switches to force Switch 1 to be the root bridge:
   - **Switch 1**. 4096
   - **Switch 2**. 12288
   - **Switch 3**. 20480

   Note: Bridge priority values are multiples of 4096.

If you do not specify a root bridge and all switches are assigned the same bridge priority value, the switch with the lowest MAC address is elected as the root bridge (see Configure and View the CST Settings on page 135).

5. On the CST Port Configuration page, select ports 1/0/1–1/0/8 and select **Enable** from the **STP Status** menu (see Configure and View the CST Port Settings on page 137).
6. Click the **Apply** button.
7. Select ports 1/0/1–1/0/5 (edge ports), and select **Enable** from the **Fast Link** menu.

   Since the edge ports are not at risk for network loops, ports with Fast Link enabled transition directly to the forwarding state.
8. Click the **Apply** button.

   You can use the CST Port Status page to view spanning tree information about each port.
9. On the MST Configuration page, create a MST instances with the following settings:
   - **MST ID**. 1
   - **Priority**. Use the default (32768)
   - **VLAN ID**. 300

   For more information, see View Rapid STP Information on page 141.
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

This appendix contains the following sections:

- Switch Default Settings
- General Feature Default Settings
- System Setup and Maintenance Settings
- Port Characteristics
- Traffic Control Settings
- Quality of Service Settings
- Security Settings
- System Management Settings
- Settings for Other Features
- Hardware Technical Specifications

Switch Default Settings

The following table describes the switch default settings.

Table 65. 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
SNTP client	Enabled
Global logging	Enabled
RAM logging	Enabled (Severity level: info and above)
Persistent (FLASH) logging	Disabled
DNS	Enabled (No servers configured)
SNMP Traps	Enabled
Auto Save	Enabled
TACACS+	Not configured
RADIUS	Not configured
Denial of service protection	Disabled
Dot1x authentication (IEEE 802.1X)	Disabled
MAC-based port security	All ports are unlocked
Access control lists (ACL)	None configured
Protected ports	None
Advertised port speed	Maximum capacity
Broadcast storm control	Disabled
MAC table address aging	300 seconds (dynamic addresses)
Default VLAN ID	1
Default VLAN name	Default

Table 65. Switch default settings (continued)

Feature	Default
Voice VLAN	Disabled
RADIUS-assigned VLANs	Disabled
Multiple Spanning Tree	Disabled
Link aggregation	No link aggregation groups (LAGs) configured
LACP system priority	32768
DiffServ	Enabled
IGMP snooping	Disabled
IGMP snooping querier	Disabled

General Feature Default Settings

The following table describes the general feature default settings.

Table 66. General feature default settings

Feature Name/Setting	Default
Virtual LAN (IEEE 802.1Q)	
Default VLANs	• 1 (Default). All ports are members. • 2 (Auto-VoIP). No ports are members. • 4089 (Auto-Video). No ports are members.
PVID	1
Acceptable Frame Types	Admit All
Ingress Filtering	Disabled
Port Priority	0
Jumbo Frames	
Frame Size	1522
Flow Control	
Admin Mode	Disabled
802.1X	
Port Based Authentication State	Disabled
VLAN Assignment Mode	Disabled

Table 66. General feature default settings (continued)

Feature Name/Setting	Default
Dynamic VLAN Creation Mode	Disabled
EAPOL Flood Mode	Disabled
Port Control	Auto
Unauthenticated VLAN ID	0 (none)
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
Forward BPDU while STP Disabled	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, 4089
STP/RSTP/MSTP, Interface	
CST STP Status	Enabled
CST Auto Edge	Enabled
CST Fast Link	Disabled

Table 66. General feature default settings (continued)

Feature Name/Setting	Default
CST BDPU Forwarding	Disabled
CST Path Cost	0
CST Priority	128
CST External Path Cost	0
Link Aggregation	
Lag Name	ch<n> where n is 1 to 8
Admin Mode	Enabled
Hash Mode	1 Src/Dest MAC, incoming port
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	Disabled
Optional TLVs	Enabled
DHCP Snooping, Global	
Admin Mode	Disabled
MAC Address Validation	Enabled
DHCP Snooping, Interface	
Trust Mode	Disabled
Logging Invalid Packets	Disabled
Rate Limit	N/A

Table 66. General feature default settings (continued)

Feature Name/Setting	Default
Burst Interval	N/A
Persistent Configuration	
Store	Local
Write Delay	300
Class of Service (CoS), Global	
Trust Mode	802.1p
802.1p to Queue Mapping (802.1p -> Queue)	0 -> 1 1 -> 0 2 -> 0 3 -> 1 4 -> 2 5 -> 2 6 -> 3 7 -> 3
DSCP to Queue Mapping (DSCP -> Queue)	Class Selector: (CS 0) 000000 -> 1 (CS 1) 001000 -> 0 (CS 2) 010000 -> 0 (CS 3) 011000 -> 1 (CS 4) 100000 -> 2 (CS 5) 101000 -> 2 (CS 6) 110000 -> 3 (CS 7) 111000 -> 3 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

Table 66. General feature default settings (continued)

Feature Name/Setting	Default
DSCP to Queue Mapping (DSCP -> Queue) (continued)	(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 (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

Table 66. General feature default settings (continued)

Feature Name/Setting	Default
DSCP to Queue Mapping (DSCP -> Queue) (continued)	(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
802.1p to Queue Mapping (802.1p –> Queue)	0 -> 1 1 -> 0 2 -> 0 3 -> 1 4 -> 2 5 -> 2 6 -> 3 7 -> 3
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	None
OUI-based priority	7
L2 Loop Protection	
Admin Mode	Disabled

System Setup and Maintenance Settings

The following table describes the system setup and maintenance settings.

Table 67. 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 68. Port characteristics

Feature	Sets Supported	Default
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	All ports	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	8 instances	Disabled

Table 68. Port characteristics (continued)

Feature	Sets Supported	Default
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 69. Traffic control settings

Feature	Sets Supported	Default
Storm control	All ports	Disabled
Jumbo frame	All ports	1522 Max = 10000 bytes

Quality of Service Settings

The following table describes the Quality of Service settings.

Table 70. 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 71. Security settings

Feature	Sets Supported	Default
802.1X	All ports	Disabled
MAC ACL	50 (100 ACLs in total, shared with IP ACLs)	All MAC addresses allowed
IP ACL	50 (100 ACLs in total, shared with MAC 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 72. 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 73. 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	8	Disabled
Filter multicast control	1	Disabled
Number of DHCP snooping bindings	8K	N/A
Number of DHCP static entries	1024	N/A

Hardware Technical Specifications

The following table describes the hardware technical specifications.

Table 74. Hardware technical specifications

Feature	Model GS308T	Model GS310TP
Network interfaces	Eight 10/100/1000BASE-T RJ-45 copper ports	• Eight 10/100/1000BASE-T RJ-45 PoE+ copper ports • Two 1000BASE-X fiber SFP ports
Power adapter	12V, 1.0A DC	54V, 1.25A DC
Power consumption	From 2.01W to 6.45W	From 3.3 to 69.3W
Switch PoE+ power budget	N/A	55W
Dimensions (W x D x H)	6.2 x 4.0 x 1.2 in. (158 x 101 x 30 mm)	9.3 x 4.0 x 1.2 in. (236 x 101 x 30 mm)
Weight	0.9 lb (0.41 kg)	1.35 lb (0.61 kg)
Operating temperature	32º to 104ºF (0° to 40°C)	
Operating humidity	90% maximum relative humidity, noncondensing	
Storage temperature	–4° to 158°F (–20º to 70ºC)	
Storage humidity	95% maximum relative humidity, noncondensing	

Table 74. Hardware technical specifications (continued)

Feature	Model GS308T Model GS310TP
Electromagnetic certifications and compliance	CE: 55032:2012 + AC:2013 / CISPR 32:2012, EN 610003-2:2014, Class B: EN 61000-3-3:2013, EN 55024:2010
	VCCI: VCCI-CISPR 32:2016, Class B
	RCM: AS/NZS CISPR 32:2013 Class B
	CCC: GB4943.1-2011, YD/T993-1998, GB/T9254-2008 (Class B)
	FCC: 47 CFR FCC Part15, Class B, ANSI C63.4:2014
	ISED: ICES-003:2016 Issue 6, Class B, ANSI C63.4:2014
	BSMI: CNS 13438 Class B
Safety certifications	CB report / certificate IEC 60950-1:2005 (ed.2) + A1:2009 + A2:2013
	UL listed (UL 1950) / cULI EC 950/EN 60950
	CE LVD: EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013
	RCM (AS/NZS) 60950.1:2015
	CCC (China Compulsory Certificate): GB4943.1-2011; YD/T993-1998; GB/T9254-2008 (Class B)
	BSMI: CNS 14336-1

For more information, see the data sheet, which you can download by visiting netgear.com/support/download/.