NETGEAR®

8-Port Multi-Gigabit Smart Managed Pro Switch with Two 10G Ports

MS510TX and MS510TXPP

User Manual

June 2018
202-11762-03

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

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

Conformity

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

Compliance

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

See the regulatory compliance document before connecting the power supply.

Do not use this device outdoors. If you connect cables or devices that are outdoors to this device, see *http://kb.netgear.com/000057103* for safety and warranty information.

Trademarks

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

Revision History

Publication Part Number	Publish Date	Comments
202-11762-03	June 2018	Updated *Configure VLAN Settings* .
202-11762-02	September 2017	Made minor changes and corrections.
202-11762-01	September 2017	First publication.

Contents

Chapter 1 Get Started

Switch Descriptions. 10
Available Publications 10
Switch Management Methods. 10
Web Browser Requirements and Supported Browsers 11
User-Defined Fields 11
Interface Naming Conventions 12
Access the Switch 12
Access the Switch On-Network With a DHCP Server. 13
Access the Switch On-Network Without a DHCP Server. 15
Access the Switch Off-Network. 16
Register the Switch 17
How to Configure Interface Settings 17
Local Browser Interface Device View. 19

Chapter 2 Configure System Information

View and Configure the Switch Management Settings 24
View or Define System Information and View Software Versions 24
View the System CPU Status. 26
View USB Device Information 27
Configure the IPv4 Address for the Network Interface and Management VLAN 28
Configure the IPv6 Address for the Network Interface 30
View the IPv6 Network Neighbor. 31
Configure the Time Settings 32
Configure DNS Settings 41
Configure Green Ethernet Settings 45
Use the Device View 50
Configure Power over Ethernet 50
PoE Overview 51
Device Class Power Requirements 51
Power Allocation and Power Budget 52
Configure the Global PoE Settings 53
Manage and View the PoE Port Configuration 55
Configure SNMP 57
Configure the SNMPv1/v2 Community 58
Configure SNMPv1/v2 Trap Settings 60
Configure SNMPv1/v2 Trap Flags 62
View the Supported MIBs 63

Configure SNMPv3 Users 64
Configure LLDP 65
Configure LLDP Global Settings 65
Configure LLDP Port Settings 67
LLDP-MED Network Policy 68
LLDP-MED Port Settings 69
Local Information 70
Neighbors Information 72
Configure DHCP Snooping 75
Configure the Global DHCP Snooping Settings 76
Enable DHCP for All Interfaces in a VLAN 77
Configure DHCP Snooping Interface Settings 77
Configure Static DHCP Bindings 78
Configure the DHCP Snooping Persistent Settings 80
Set Up PoE Timer Schedules 80
Create a PoE Timer Schedule 81
Specify the Settings for a PoE Timer Schedule 82
Add a Periodic Schedule for a PoE Timer Schedule 83
Delete a Periodic Schedule for a PoE Timer Schedule 84
Delete a PoE Timer Schedule 85

Chapter 3 Configure Switching

Configure Port Settings and Flow Control 87
Configure IEEE 802.3x Global Flow Control 87
Configure the Port Settings 88
Configure Link Aggregation Groups 89
Configure LAG Settings 90
Configure LAG Membership 92
Set the LACP System Priority 93
Set the LACP Port Priority Settings 93
Configure VLANs 94
Configure VLAN Settings 95
Configure VLAN Membership 97
View VLAN Status 99
Configure Port PVID Settings 100
Configure MAC-Based VLAN Groups 102
Manually Add Members to or Remove Them From a MAC-Based VLAN Group 104
Configure Protocol-Based VLAN Groups 104
Manually Add Members to or Remove Them From a Protocol-Based VLAN Group 106
Configure GARP Switch Settings 107
Configure GARP Ports 108
Configure a Voice VLAN 110
Configure the Global Voice VLAN Settings 110
Configure Membership for the Voice VLAN 111
Manage the OUI Table 112

Configure Auto-VoIP 114
Configure Spanning Tree Protocol 115
Configure STP Settings 116
Configure CST Settings 118
Configure CST Port Settings 120
View the CST Port Status 121
View Rapid STP Information 123
Manage MST Settings 124
Configure MST Port Settings 126
View STP Statistics 129
Configure Multicast 129
View the MFDB Table 130
View the MFDB Statistics 132
Configure Auto-Video 132
IGMP Snooping Overview 133
Configure the Global IGMP Snooping Settings 134
View the IGMP Snooping Table 135
Configure IGMP Snooping for VLANs 136
Modify IGMP Snooping Settings for a VLAN 137
Disable IGMP Snooping on a VLAN and Remove It From the Table 138
IGMP Snooping Querier Overview 138
Configure IGMP Snooping Querier 139
Configure IGMP Snooping Querier for VLANs 140
Display the IGMP Snooping Querier for VLAN Status 141
MLD Snooping Overview 142
Configure the Global MLD Snooping Settings 142
Configure MLD Snooping for a VLAN 143
Configure a Multicast Router Interface on a VLAN 144
Configure MLD Snooping Querier 145
Configure MLD Snooping Querier VLAN Settings 146
Configure a Multicast Group 147
Remove a Multicast Group 148
Configure Multicast Group Membership 149
Configure the Multicast Forward All Option 150
View, Search, and Manage the MAC Address Table 151
View and Search the MAC Address Table 152
Change the Aging-Out Period of Dynamic MAC Addresses 153
Add a Static MAC Address 154
Remove a Static MAC Address 154

Chapter 4 Configure Routing

IP Routing Overview 157
Configure IP Settings 157
Configure the Routing Settings 157
View the IP Statistics 158
Configure VLAN Routing 161
Use the VLAN Static Routing Wizard 162
VLAN Routing Configuration 163

Manage IPv4 Routes 164
Configure Address Resolution Protocol 166
Display the ARP Cache 167
Add an Entry to the ARP Table 168
Configure the Global Aging-Out Time for ARP 169
Remove an ARP Entry From the ARP Cache 170
Configure IPv6 171
Configure IPv6 Global Settings 171
Add a Static IPv6 Route 172
Change the Preference for a Static IPv6 Route 173
Remove a Static IPv6 Route 174
View the IPv6 Route Table 175
Configure IPv6 VLAN Interface Settings 176
Add an IPv6 Global Address to an IPv6 VLAN 178
Change the Settings for an IPv6 Global Address on an IPv6 VLAN 180
Remove an IPv6 Global Address From an IPv6 VLAN 181
Add an IPv6 Prefix for Advertisement on an IPv6 VLAN 181
Change the Settings for an IPv6 Prefix for Advertisement on an IPv6 VLAN 183
Remove an IPv6 Prefix From an IPv6 VLAN 183
View IPv6 Statistics for an Interface 184
View or Clear the IPv6 Neighbor Table 186

Chapter 5 Configure Quality of Service

Manage Class of Service 189
CoS Configuration 189
Configure Global CoS Settings 190
Configure CoS Interface Settings for an Interface 190
Configure the Global CoS Queue Settings 192
Configure the Global 802.1p to Queue Mapping 193
DSCP to Queue Mapping 194
Manage Differentiated Services 195
DiffServ Overview 196
View the Global DiffServ Resources 197
Specify DSCP Remark Values for Violate Action IP Packets 197
Configure IPv4 DiffServ Classes 199
Configure an IPv6 DiffServ IPv6 Classes 203
Configure a DiffServ Policy 207
Configure DiffServ Service Interfaces 212
View DiffServ Service Statistics 213

Chapter 6 Manage Device Security

Management Security Settings 216
Change the Password 216
Reset the Password to the Factory Default Value 217
Configure RADIUS Servers 218
Configure TACACS+ Servers 224

Configure Authentication Lists 227
Configure Management Access 230
Configure HTTP Settings 231
Configure HTTPS Settings 231
Manage the Certificate 233
Configure Access Control 235
Configure Port Authentication 241
Configure Global 802.1X Settings 241
Manage Port Authentication 243
View the Port Summary 245
View the Client Summary 247
Set Up Traffic Control 248
Configure Storm Control 248
Configure Port Security 249
Configure Protected Ports 252
Configure Private VLANs 252
Configure Access Control Lists 258
Use the ACL Wizard to Create a Simple ACL 259
Configure a Basic MAC ACL 264
Configure MAC ACL Rules 266
Configure MAC Bindings 270
View or Delete MAC ACL Bindings in the MAC Binding Table 271
Configure an IP ACL 272
Configure Rules for a Basic IP ACL 274
Configure Rules for an Extended IP ACL 277
Configure an IPv6 ACL 281
Configure IPv6 Rules 283
Configure IP ACL Interface Bindings 286
View or Delete IP ACL Bindings in the IP ACL Binding Table 288

Chapter 7 Monitor the System

Monitor the Switch and the Ports 291
Switch Statistics 291
View Port Statistics 292
View Detailed Port Statistics 295
View EAP Statistics 298
Perform a Cable Test 300
Configure and View Logs 301
Manage the Buffered Logs 302
Manage the Flash Log 303
Manage the Server Log 305
View the Trap Logs 307
Configure Port Mirroring 308
View the System Resource Utilization 309

Chapter 8 Maintain the Switch and Perform Troubleshooting

Reboot the Switch 312

Reset the Switch to Its Factory Default Settings 312
Export a File From the Switch 313
Export a File to the TFTP Server 313
HTTP File Export 315
Export a File From the Switch to a USB Device 316
Download a File to the Switch 317
Download a File to the Switch Using TFTP 317
Download a File to the Switch Using HTTP 319
Download a File From a USB Device 320
Manage Files 321
Change the Image That Loads During the Boot Process 321
View the Dual Image Status 322
Troubleshooting 323
Ping an IPv4 Address 323
Ping an IPv6 Address 325
Send an IPv4 Traceroute 326
Send an IPv6 Traceroute 327
Generate Technical Support Information 328
Enable Remote Diagnostics 329

Appendix A Configuration Examples

Virtual Local Area Networks (VLANs) 331
VLAN Configuration Examples 332
Access Control Lists (ACLs) 333
Sample MAC ACL Configuration 333
Sample Standard IP ACL Configuration 334
Differentiated Services (DiffServ) 335
Class 336
DiffServ Traffic Classes 336
Creating Policies 337
DiffServ Example Configuration 338
802.1X 339
802.1X Example Configuration 341
MSTP 342
MSTP Example Configuration 344
VLAN Routing Interface Configuration Example 346

Appendix B Hardware Specifications and Default Settings

Hardware Specifications 348
Switch Default Settings 349

Get Started

1

This manual describes how you can configure and monitor the following NETGEAR switches by using the local browser–based management interface:

- **MS510TX**. 8-Port Multi-Gigabit Smart Managed Pro Switch with two 10G Ports, Model MS510TX
- **MS510TXPP**. 8-Port Multi-Gigabit Smart Managed Pro Switch with PoE+ and two 10G Ports, Model MS510TXPP

This chapter contains the following sections:

- *Switch Descriptions*
- *Available Publications*
- *Switch Management Methods*
- *Web Browser Requirements and Supported Browsers*
- *User-Defined Fields*
- *Interface Naming Conventions*
- *Access the Switch*
- *Register the Switch*
- *How to Configure Interface Settings*
- *Local Browser Interface Device View*

In this manual, we refer to both switch models as *the switch*. Unless noted otherwise, all information applies to both switch models.

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

Firmware updates with new features and bug fixes are automatically made available through the Insight app and, if selected, pushed straight from the cloud to the device. If you are not using the Insight app to manage your device, you can manually download and install the latest firmware by visiting *downloadcenter.netgear.com*. If the features or behavior of your product does not match what is described in this manual, you might need to update your firmware.

Switch Descriptions

The switch provides four multispeed Gigabit Ethernet and four 1G Ethernet RJ-45 copper ports with one dedicated 10G RJ-45 copper uplink port and one dedicated SFP+ fiber uplink port that supports 10G and 1G. Two of the four multispeed ports support 5G, 2.5G, and 1G. The other two multispeed ports support 2.5G and 1G. (The 10G RJ-45 copper uplink port also supports 5G, 2.5G and 1G.)

The switch models differ in the following ways:

- **Model MS510TXPP**. This model supports Power over Ethernet plus (PoE+) on all four multispeed ports and four 1G ports so that you can let the switch provide power to PoE-capable devices such as WiFi access points, VoIP phones, and IP security cameras.
- **Model MS510TXPP**. This model can supply up to 30W PoE+ (IEEE 802.3at) to each port, with a maximum PoE power budget of 180W across all active PoE+ ports.

Available Publications

The following guides and manual are available at *downloadcenter.netgear.com*:

- *Installation Guide*
- *Hardware Installation Guide*
- *Smart Control Center User Manual*

For general switch information, see the NETGEAR knowledge base articles at *netgear.com/support*.

Switch Management Methods

If you prefer, you can use the switch as a plug-and-play device, so you do not need to set up a custom configuration. Just connect power, connect to your network and to your other devices, and you are done.

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.

You can configure and monitor the switch by using one of the following methods:

- **Smart Control Center (SCC)**. Initial discovery of the switch on the network requires the Smart Control Center (SCC) program, which runs on a Windows-based computer and is included on the resource CD. You can also download the SCC program from *downloadcenter.netgear.com*. If you do not use a Windows-based computer, get the IP address of the switch from the DHCP server in the network or use an IP scanner utility.

  After discovery, you can configure the switch using the local browser–based management interface, or the SCC program for very basic setup. For more information, see *Access the Switch* on page 12 and the SCC user manual, which you can download from *downloadcenter.netgear.com*.

- **Local browser–based management interface**. This manual describes how to use the local browser–based management interface, in this manual referred to as the local browser interface, to manage and monitor the switch. The local browser interface lets you configure basic and advanced features. For more information, see *Access the Switch* on page 12.
- **Simple Network Management Protocol (SNMP)**. You can manage through switch through SNMP. For more information, see *Configure SNMP* on page 57.

Web Browser Requirements and Supported Browsers

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

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

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

- Microsoft Internet Explorer (IE) versions 9–11
- Microsoft Edge 25
- Mozilla Firefox versions 53–54
- Chrome versions 58–59
- Safari on MAC OS: 10.1 (MAC OS Yosemite Version 10.10.5)

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 1. Invalid characters for user-defined fields

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

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 local browser interface.

The following types of ports are supported:

- Ports g1-g4 are Gigabit ports.
- Ports mg5-mg6 are Multi-Gigabit Ethernet ports, each of which supports a maximum speed of 2.5 Gbps.
- Ports mg7-mg8 are Multi-Gigabit Ethernet ports, each of which supports a maximum speed of 5 Gbps.
- Port xmg9 is a Multi-Gigabit Ethernet port that supports a maximum speed of 10 Gbps.
- Port xg10 is a fiber port in which you can install an SFP+ module.

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

Table 2. Naming conventions for interfaces

Interface	Description	Examples
Physical	The physical ports are numbered sequentially starting from one.	g1, g2, mg5, xmg9 xg10
Link aggregation group (LAG)	LAG interfaces are logical interfaces that are used only for bridging functions.	LAG1, LAG2, LAG8
Routing VLAN interfaces	An interface is used for routing functionality.	VLAN 1, VLAN 2, VLAN 55

Access the Switch

For easiest access, we recommend that you connect 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 (see *Access the Switch On-Network With a DHCP Server* on page 13). If your network does not include a DHCP server, you can assign a static IP address (see *Access the Switch On-Network Without a DHCP Server* on page 15).

It is also possible to configure the switch connected directly only to the computer that you are using to configure it, and not connected to the network (off-network, see *Access the Switch Off-Network* on page 16).

Use *one* of the following methods to determine or assign the IP address of the switch and access the switch:

- **Determine the DHCP-assigned IP address**. 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 *Access the Switch On-Network With a DHCP Server* on page 13.

- **Assign a static IP address through the Smart Control Center**. If you connect the switch to a network that does not include a DHCP server, or you prefer to assign static addresses, you can use the Smart Control Center (SCC) to assign a static IP address, subnet mask, and default gateway. For more information, see *Access the Switch On-Network Without a DHCP Server* on page 15.
- **Assign a static IP address from a directly-connected computer**. If you do not use the Smart Control Center to assign a static address, you can connect to the switch directly 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 more information, see *Access the Switch Off-Network* on page 16.

Access the Switch On-Network With a DHCP Server

The DHCP client on the switch is enabled by default, allowing a DHCP server on the network (or router that functions as a DHCP server) to assign an IP address to the switch.

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.

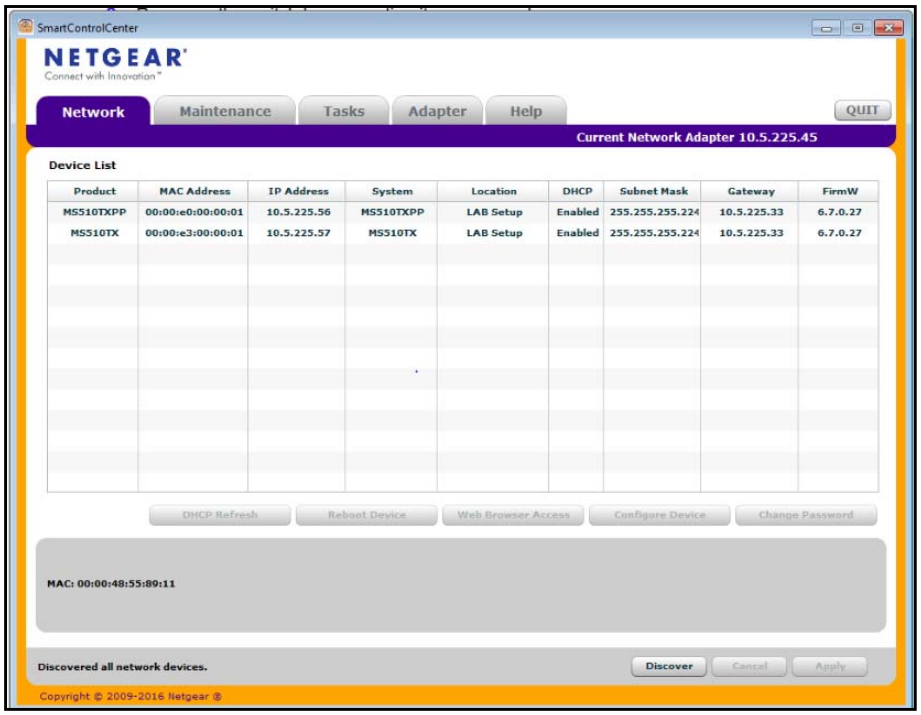
The SCC program runs on a Windows-based computer and is included on the resource CD. You can also download the SCC program from *downloadcenter.netgear.com*. If you do not use a Windows-based computer, get the IP address of the switch from the DHCP server in the network or use an IP scanner utility, which are available free of charge on the Internet.

Note: The computer that is running the SCC program must be on the same network (that is, in the same broadcast domain) as the switch.

➢ **To determine the DHCP-assigned IP address of the switch and access the switch:**

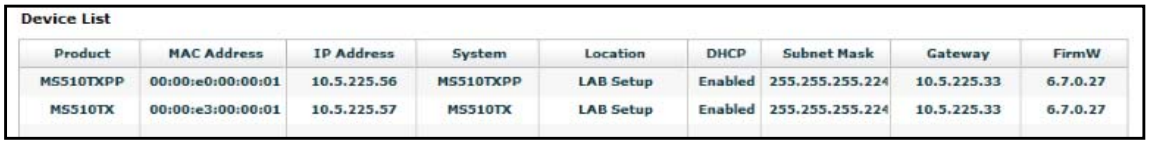
1. Connect the switch to a network that includes a DHCP server.
2. Power on the switch by connecting its power cord.
3. Install the Smart Control Center on your computer.
4. Start the Smart Control Center.
5. Click the **Discover** button.

   The Smart Control Center finds your switch.



6. Write down the displayed IP address assigned by the DHCP server.

   You need this address later to access the switch directly from a web browser (without using the Smart Control Center).



7. Select the switch by clicking the row for the switch.
8. Click the **Web Browser Access** button.

   The Smart Control Center launches a browser.

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

   The default password is **password**.

   The Switch Information page displays. You can now configure the switch.

Access the Switch On-Network Without a DHCP Server

You can use the Smart Control Center (SCC) to set up your switch in a network without a DHCP server and assign a static IP address to the switch.

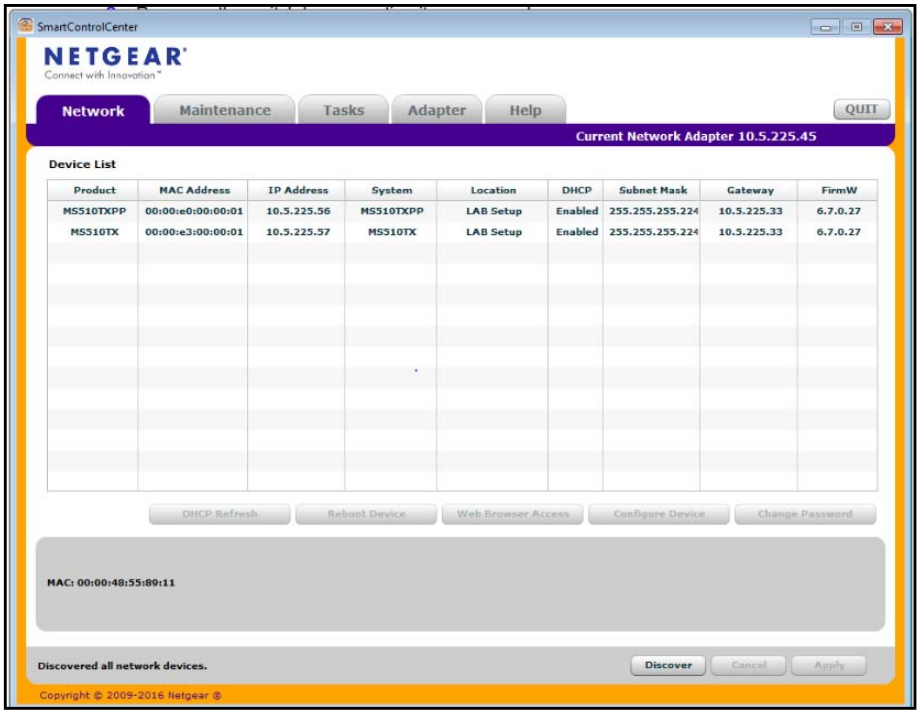
If you prefer, you can assign the switch a static IP address even if your network does include a DHCP server.

The SCC program runs on a Windows-based computer and is included on the resource CD. You can also download the SCC program from *downloadcenter.netgear.com*. If you do not use a Windows-based computer, see *Access the Switch Off-Network* on page 16.

➢ **To assign a static IP address to the switch on-network and access the switch:**

1. Connect the switch to a 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.

   The Smart Control Center finds your switch.



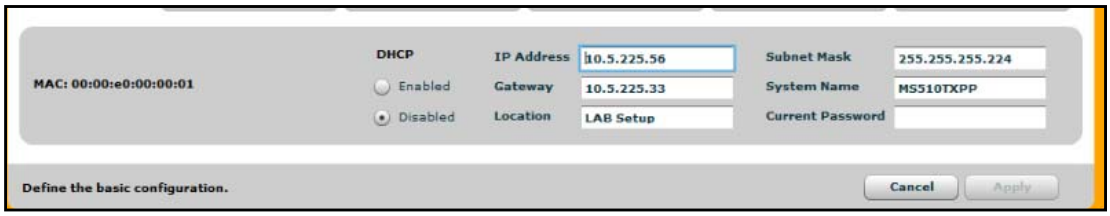
6. Select the switch, and then click the **Configure Device** button.

   The page expands to display additional fields at the bottom.

7. Select the **Disabled** radio button.

   The DHCP client is disabled.

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



9. Enter the switch password to continue with the configuration change.

   The default password is **password**. You must enter the password each time that you use the Smart Control Center to update the switch settings.

   Note: If you change the default password to a custom password (which we recommend) using the local browser interface and need to use the Smart Control Center again, you must enter the custom password for configuration changes to be accepted.

10. Click the **Apply** button.

    Your settings are saved.

11. Click the **Discover** button.

    The Smart Control Center finds your switch with its new IP address.

12. Select the switch by clicking the row for the switch.
13. Click the **Web Browser Access** button.

    The Smart Control Center launches a browser.

    The login window opens.

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

    The default password is **password**.

    The Switch Information page displays. You can now configure the switch.

Access the Switch Off-Network

You can connect to the switch directly from a computer and change the settings by using the local browser interface of the switch. The default IP address of the switch is 192.168.0.239. The IP address of the computer that you use to access the switch must in the same subnet as the default IP address of the switch, that is, it must be in the in the 192.168.0.0/24 subnet.

➢ **To assign a static IP address to the switch off-network from a directly-connected computer:**

1. Record your computer's TCP/IP configuration settings, and then configure the computer with a static IP address.

For example, configure 192.168.0.210 as the IP address and 255.255.255.0 as the subnet mask.

Note: If you are unsure how to do this, visit *netgear.com/search-support.aspx* and search for the following:
How to set a static IP address in Windows
or
Setting a static IP address on your network adapter in Mac OS

2. Plug the switch into a power outlet and then connect your computer to the switch using an Ethernet cable.

   You can connect the Ethernet cable to any Ethernet port on the switch.

3. Open a web browser, and enter **http://192.168.0.239**.

   This is the default address of the switch.

   The login window opens.

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

   The default password is **password**.

   The Switch Information page displays. You can now configure the switch.

5. After you complete the configuration of the switch, reconfigure the computer that you used for this process to its original TCP/IP settings.

   You can now connect your switch to your network using an Ethernet cable.

Register the Switch

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

When you log in to the switch, you are prompted to register with NETGEAR. However, at any time you can visit the NETGEAR website for registration at *https://my.netgear.com/register/register.aspx*.

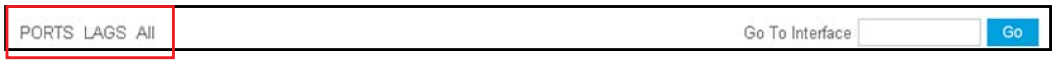
How to Configure Interface Settings

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 **PORTS** link.
- To display all LAGs, click the **LAGS** 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 Switch* on page 12.

➢ **To configure a single port or LAG:**

1. Click the **All** link to display the all ports and LAGs.
2. Do one of the following:
   a. In the **Go To Interface** field, type the port number and click the **Go** button.

      For example, type **g4** for a port or type **LAG2** for a LAG. For more information, see *Interface Naming Conventions* on page 12.

      The check box for the interface is selected, the row for the selected interface is highlighted, and the interface number displays in the heading row.

   b. Select the check box for the port or LAG.

      The row for the selected interface is highlighted, and the interface number displays in the heading row.
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 next to each port and LAG 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 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 boxes for all ports and LAGs are 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.

Local Browser Interface Device View

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

➢ **To use the 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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The Switch Information page displays.
5. Select **System > Device View**.

The previous figure shows the Device View page for model MS510TX.

The system LEDs are located on the left side.

Depending upon the status of the port, the port color in Device View is either yellow, green, or black (that is, off).

The following table describes the LEDs on the Device View page.

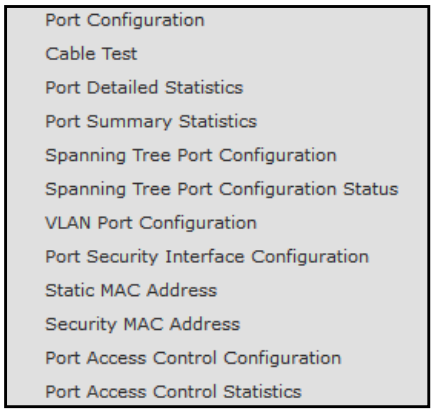
Table 3. LEDs on the Device View page

LED	Description
Power LED	The Power LED is a bicolor LED that serves as an indicator of power and diagnostic status: • **Solid green**. Power is supplied to the switch and the switch is operating normally. • **Solid yellow**. The switch is in the boot-up stage. • **Off**. No power is supplied to the switch.
Fan LED	The Fan LED indicates the following status: • **Off**. Fan is operating normally. • **Solid yellow**. A problem occurred with the fan.
PoE MAX LED (Model MS510TXPP only)	The PoE MAX Power LED indicates the following PoE conditions at switch (not port) level: • **Off**. More than 7W of PoE power is available for another powered device (PD). • **Solid yellow**. Less than 7W of PoE power is available for another PD. • **Blinking yellow**. The PoE Max LED was activate in the previous two minutes.
1G Ports 1–4, Left LEDs Link, speed, and activity	The left LEDs for ports 1–4 (g1 to g4) indicate the following status: • **Off**. No link is established. • **Solid green**. A valid 1 Gbps link is established. • **Blinking green**. The port is transmitting or receiving packets at 1 Gbps. • **Solid yellow**. A valid 10 Mbps or 100 Mbps link is established. • **Blinking yellow**.The port is transmitting or receiving packets at 10 Mbps or 100 Mbps.
1G Ports 1–4, Right LEDs PoE status (Model MS510TXPP only)	The right LEDs for ports 1–4 (g1 to g4) indicate the following status: • **Off**. The port is not delivering PoE. • **Solid green**. The port is delivering PoE. • **Solid yellow**. A PoE fault occurred.
2.5G Ports 5 and 6, Left LEDs Link, speed, and activity	The left LEDs for ports 5 and 6 (mg5 and mg6) indicate the following status: • **Off**. No link is established. • **Solid green**. A valid 2.5 Gbps link is established. • **Blinking green**. The port is transmitting or receiving packets at 2.5 Gbps. • **Solid yellow**. A valid 100 Mbps or 1000 Mbps link is established. • **Blinking yellow**. The port is transmitting or receiving packets at 100 Mbps or 1000 Mbps.

Table 3. LEDs on the Device View page (continued)

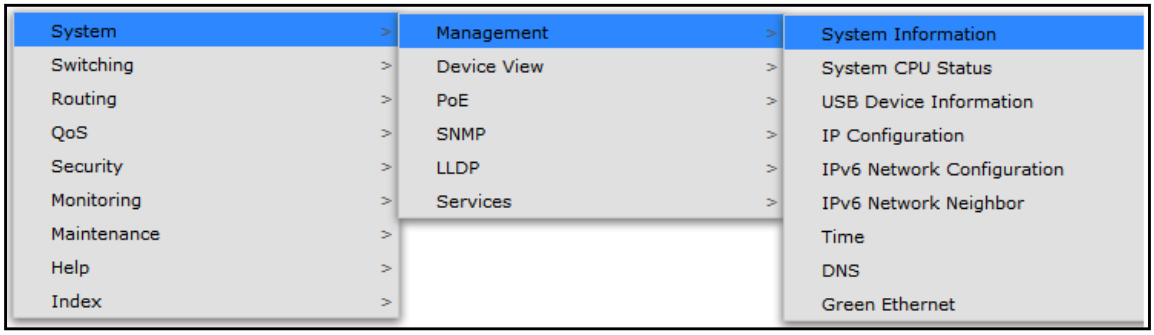
LED	Description
2.5G Ports 5 and 6, Right LEDs PoE status (Model MS510TXPP only)	The right LEDs for ports 5 and 6 (mg5 and mg6) indicate the following status: • **Off**. The port is not delivering PoE. • **Solid green**. The port is delivering PoE. • **Solid yellow**. A PoE fault occurred.
5G Ports 7 and 8, Left LEDs Link, speed, and activity	The left LEDs for ports 7 and 8 (mg7 and mg8) indicate the following status: • **Off**. No link is established. • **Solid green**. A valid 2.5 Gbps or 5 Gbps link is established. • **Blinking green**. The port is transmitting or receiving packets at 2.5 Gbps or 5 Gbps. • **Solid yellow**. A valid 100 Mbps or 1000 Mbps link is established. • **Blinking yellow**. The port is transmitting or receiving packets at 100 Mbps or 1000 Mbps.
5G Ports 7 and 8, Right LEDs PoE status (Model MS510TXPP only)	The right LEDs for ports 7 and 8 (mg7 and mg8) indicate the following status: • **Off**. The port is not delivering PoE. • **Solid green**. The port is delivering PoE. • **Solid yellow**. A PoE fault occurred.
10G Port 9, LED Link, speed, and activity	The LED for port 9 (xmg9) indicates the following status: • **Off**. No link is established. • **Solid green**. A valid 10 Gbps link is established. • **Blinking green**. The port is transmitting or receiving packets at 10 Gbps. • **Solid yellow**. A valid 5 Gbps, 2.5 Gbps, 1000 Mbps, or 100 Mbps link is established. • **Blinking yellow**. The port is transmitting or receiving packets at 5 Gbps, 2.5 Gbps, 1000 Mbps, or 100 Mbps
SFP+ Port 10, LEDs Link, speed, and activity	The LEDs for port 10 (xg10, the SFP+ port) indicate the following status: • **Off**. No SFP+ module link is established on the fiber port. • **Left LED solid green**. The fiber port established a valid 10 Gbps link. • **Left LED blinking green**. The fiber port is transmitting or receiving packets at 10 Gbps. • **Right LED solid yellow**. The fiber port established a valid 1 Gbps link. • **Right LED blinking yellow**. The fiber port is transmitting or receiving packets at 1 Gbps

6. To see a menu that displays statistics and configuration options, right-click a port.



The previous figure shows the Device View page for model MS510TXPP.

7. To display the main menu that contains the same options as the navigation menu at the top of the page, right-click the graphic without clicking a specific port.



The previous figure shows the Device View page for model MS510TXPP.

Configure System Information

2

This chapter covers the following topics:

- *View and Configure the Switch Management Settings*
- *Use the Device View*
- *Configure Power over Ethernet*
- *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 management interface IP address, system clock settings, and DNS information. From the **System > Management** menu, you can access pages that are described in the following sections:

- *View or Define System Information and View Software Versions* on page 24
- *View the System CPU Status* on page 26
- *View USB Device Information* on page 27
- *Configure the IPv4 Address for the Network Interface and Management VLAN* on page 28
- *Configure the IPv6 Address for the Network Interface* on page 30
- *View the IPv6 Network Neighbor* on page 31
- *Configure the Time Settings* on page 32
- *Configure DNS Settings* on page 41
- *Configure Green Ethernet Settings* on page 45

View or Define System Information and View Software Versions

When you log in, the System Information page displays. Use this page to configure and view general device information such as system name, location, and contact, general system temperature, temperatures of the fans, and boot and software versions.

➢ **To view or define system information and view 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.

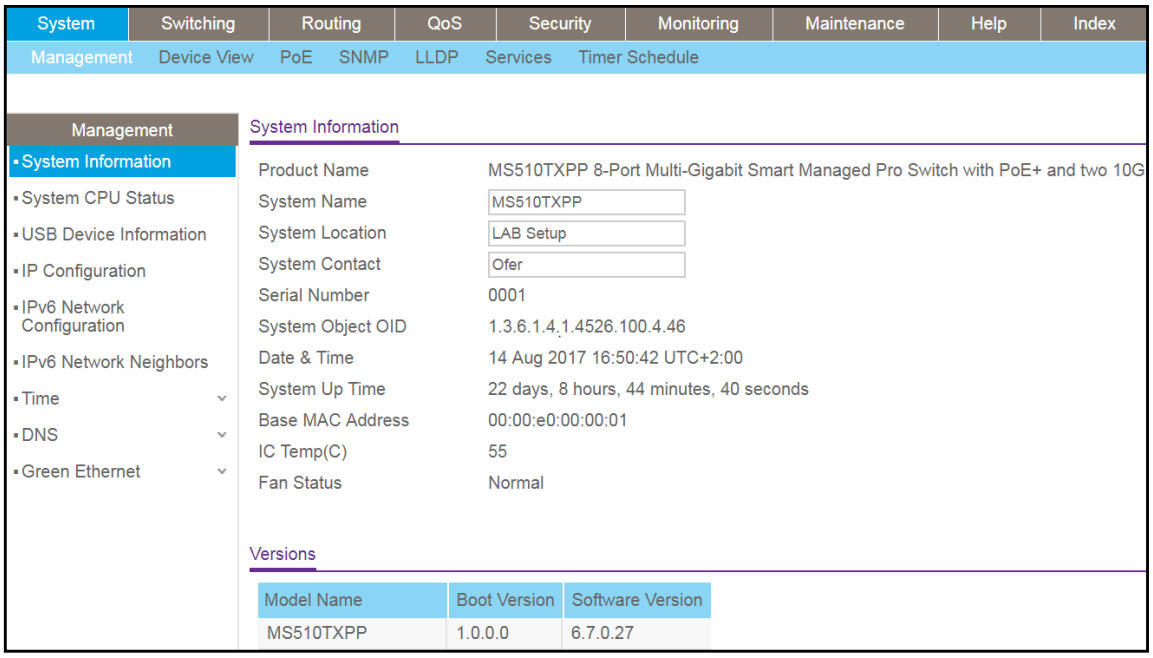
   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   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. 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.

Field	Description
Serial Number	The serial number of the switch.
System Object ID	The base object ID for the switch's enterprise MIB.
Date & Time	The current date and time.
System Up Time	The number of days, hours, minutes, and seconds since the last system restart.
Base MAC Address	Universally assigned network address.
IC Temp(C)	Integrated circuit temperature in Celsius values.
Fan Status	The status of fan operations.
Model Name	The model name of the switch.

Field	Description
Boot Version	The boot code version of the switch.
Software Version	The software version of the switch.

View the System CPU Status

Use the System CPU Status page to monitor the CPU, memory resources, and utilization patterns across various intervals to assess the performance of the switch.

➢ **To configure and view the system CPU status and utilization:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The CPU Memory Status page displays.

   The page shows the total system memory and the available memory in MB.

6. Enable the switch to calculate the CPU utilization:
   - **CPU Utilization**. Select the **Disable** or **Enable** radio button. By default, the **Enable** radio button is selected.
   - **Refresh Rate**. Select a radio button number to specify the number of seconds at which the CPU utilization is computed. By default, the **No** radio button is selected.

   The CPU Input Rate field shows the number of frames forwarded to the CPU per second.

   The CPU utilization rate is displayed in a graph. The Y axis represents the CPU utilization in percentage. The X axis represents the number of elapsed seconds and is correlated to the selected refresh rate.

View USB Device Information

Use the USB Device Information page to display the USB device status, memory statistics, and directory details.

The limitations for the USB device supported on the switch are as follows:

- The USB disk must comply with the USB 2.0 standard.
- The USB disk must be file type FAT32. File type NTFS is not supported.

➢ **To display the USB device information:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > Management > USB Device Information**.

   The USB Memory Statistics page displays.

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

The following table describes the USB Memory Statistics information.

Table 4. USB Memory Statistics information

Field	Description
Total Size	The USB flash device storage size in bytes.
Bytes Used	The size of memory used on the USB flash device.
Bytes Free	The size of memory free on the USB flash device.

The following table describes the USB Directory Details information.

Table 5. USB Directory Details information

Field	Description
File Name	The name of the file stored in the USB flash drive.
Type	The type of file, which can be one of the following: • **Folder**. A subfolder within the file. Click the folder name to view the contents of the subfolder. • **File**. A file. • **Other**. A path, which can be one of the following: - **Current path**. The full path for the folder that is being displayed. - **Parent folder path**. The path for the parent folder of the folder that is being displayed. You can click the entry and open the parent folder.
File Size	The size, in bytes, of the file stored in the USB flash drive.
Modification Time	The last modification time of the file stored in the USB flash drive.

Configure the IPv4 Address for the Network Interface and Management VLAN

You can configure network information for the network interface, which is the logical interface used for in-band connectivity with the switch through any of the switch's ports. You also use the IPv4 address of the network interface to connect to the switch through the local browser interface. The configuration parameters that is associated with the switch's network interface do not affect the configuration of the ports through which traffic is switched.

➢ **To configure the IPv4 address for the network interface and the management 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The IP Configuration page displays.

6. Select a radio button to determine how to configure the network information for the switch management interface:
   - **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 (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. 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. The factory default IP address is 192.168.0.239.
   - **Subnet Mask**. The IP subnet mask for the interface. The factory default subnet mask is 255.255.255.0.
   - **Default Gateway**. The default gateway for the IP interface. The factory default gateway address is 192.168.0.254.
8. From the **Management VLAN ID** menu, select the VLAN ID for the management VLAN.

   The management VLAN is used to establish an IP connection to the switch from a computer that is connected to a port in the same VLAN. 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 94.

   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 IPv6 Address for the Network Interface

You can configure the IPv6 address for the network interface, which is the logical interface used for in-band connectivity with the switch through any of the switch's front-panel ports. You also use the IPv6 address of the network interface to connect to the switch through the local browser interface. The configuration parameters that is associated with the switch's network interface do not affect the configuration of the ports through which traffic is switched.

To access the switch over an IPv6 network, you must initially configure the switch with IPv6 information (IPv6 prefix, prefix length, and default gateway). IPv6 can be configured using any of the following options:

- IPv6 autoconfiguration
- DHCPv6

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

➢ **To configure the IPv6 address for the network 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > Management > IPv6 Network Configuration**.

   The IPv6 Network Global Configuration page displays.

6. Ensure that the Admin Mode **Enable** radio button is selected.
7. Select IPv6 Address Auto Configuration Mode **Enable** radio button to enable the network interface to acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of router advertisement messages.

   When this mode is disabled, the network interface does not use the native IPv6 address autoconfiguration features to acquire an IPv6 address.

8. In the **Current Network Configuration Protocol** field define the IPv6 network interface to receive an IPv6 address from a DHCP server. The default value is None.
9. If the above field is set to DHCPv6 Protocol, the **DHCPv6 Client DUID** field (read only) displays the DHCPv6 client DUID

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

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

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

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

       The address is in the global address format.

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

    c. Click the **Add** button.

12. Click the **Apply** button.

    Your settings are saved.

View the IPv6 Network Neighbor

Use the IPv6 Network Neighbor page to view information about the IPv6 neighbors that the switch discovers through the network interface by using the Neighbor Discovery Protocol (NDP).

➢ **To view the IPv6 neighbor table:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > Management > IPv6 Network Neighbor**.

   The IPv6 Network Interface Neighbor Table page displays.

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

Table 6. IPv6 network interface neighbor table information

Field	Description
IPv6 Address	The IPv6 address of a neighbor switch visible to the network interface.
MAC Address	The MAC address of a neighbor switch.
isRtr	• **True**. The neighbor machine is a router. • **False**. The neighbor machine is not a router.
Neighbor State	The state of the neighboring switch: • **Reach**. No more than ReachableTime milliseconds elapsed since the switch received confirmation that the forward path to the neighbor was functioning properly. In the Reach state, the device takes no special action when packets are sent. • **Stale**. More than ReachableTime milliseconds elapsed since the switch received confirmation that the forward path was functioning properly. In the Stale state, the device takes no action until a packet is sent. • **Delay**. More than ReachableTime milliseconds elapsed since the switch received confirmation that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the Delay state, the device sends a neighbor solicitation message and changes the state to Probe. • **Probe**. The switch actively seeks confirmation by repeatedly sending neighbor solicitation messages each RetransTimer milliseconds until a confirmation is received.
Last Updated	The last time that the neighbor was updated.

Configure the Time Settings

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

Configure the Time Setting Manually

Use the Time Configuration page to 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 *Access the Switch* on page 12.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The Time Configuration page displays.

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

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

9. Click the **Apply** button.

   Your settings are saved.

Configure 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The SNTP Server Configuration page displays. The page also displays the SNTP Server Status section.

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

   The address can be either an IP address (IPv4, IPv6) or a host name (DNS). The default value is IPv4.

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

   Unicast SNTP requests are sent to this address. If this address is a DNS host name, then that host name is resolved into an IP address each time an SNTP request is sent to it.

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

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

9. Click the **Add** button.

The SNTP server entry is added.

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

    You can configure up to eight 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 7. 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.

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 *Access the Switch* on page 12.

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

   The default password is **password**.

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

   The SNTP Server Configuration page displays.
6. Select the check box for 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 *Access the Switch* on page 12.

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

   The default password is **password**.

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

   The SNTP Server Configuration page displays.
6. Select the check box for the configured server to remove.
7. Click the **Delete** button.

   The entry is removed, and the device is updated.

Enable SNTP and Configure the Time Zone Offset

You must first configure an SNTP server (see *Configure an SNTP Server* on page 33) before you can enable SNTP.

➢ **To enable SNTP settings and configure the time zone offset:**

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

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

   The default password is **password**.

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

The Time Configuration page displays.

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

   The **Date** and **Time** fields are disabled because the switch receives the date and time from the network.

7. From the **Time Zone Offset** menu, select the number of hours that the time zone in which the switch is located differs from the Coordinated Universal Time (UTC).

   The time zone can affect the display of the current system time. The default value is UTC 0:00.

   Note: When you use SNTP/NTP time servers to update the switch's clock, the time data received from the server is based on the UTC 0:00, which is the same as Greenwich Mean Time (GMT). This might not be the time zone in which the switch is located.

8. Click the **Apply** button.

   Your settings are saved.

9. To refresh the page, click the **Refresh** button.

View SNTP Global Status

You can view global SNTP status information.

➢ **To view SNTP global status:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > Management > Time > SNTP Global Status**.

   The SNTP Global Status page displays.

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

The following table displays the nonconfigurable SNTP Global Status information.

Table 8. 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.
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.
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.

Configure Daylight Saving Time Settings

Use the Daylight Saving Time Configuration page to configure settings for daylight saving time, which is also known as summer time. Used in some countries around the world, daylight saving 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 *Access the Switch* on page 12.

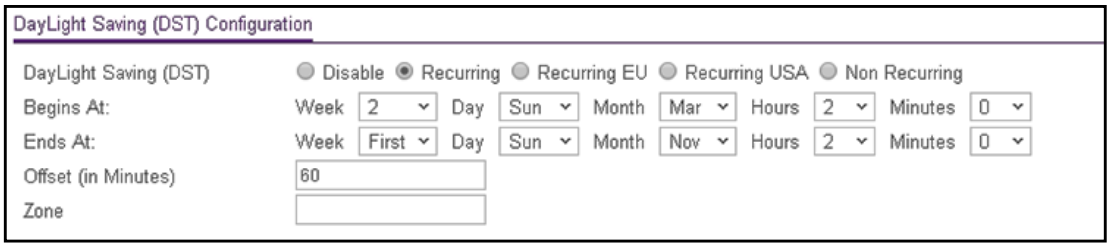
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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



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 daylight saving 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 daylight saving time settings do not repeat on an annual basis.

   If you select any radio button other than the **Disable** radio button (which is the default selection), the page adjusts to display additional fields.

7. Configure how the daylight saving settings recur as described in the following table.

Field	Description
Begins At **Note:** These fields do not apply if you select the **Recurring EU** radio button or the **Recurring USA** radio button.	If you select the **Recurring** radio button, specify the start date and time of daylight saving time in the following fields: • **Week**. Configure the start week. • **Day**. Configure the start day. • **Month**. Configure the start month. • **Hours**. Configure the start hour. • **Minutes**. Configure the start minute. If you select the **Non Recurring** radio button, specify the start date and time of daylight saving in the following fields: • **Year**. Configure the start year. • **Date**. Configure the start date. • **Month**. Configure the start month. • **Hours**. Configure the start hour. • **Minutes**. Configure the start minute.

Field	Description
Ends At **Note:** These fields do not apply if you select the **Recurring EU** radio button or the **Recurring USA** radio button.	If you select the **Recurring** radio button, specify the end date and time of daylight saving in the following fields: • **Week**. Configure the end week. • **Day**. Configure the end day. • **Month**. Configure the end month. • **Hours**. Configure the end hour. • **Minutes**. Configure the end minute. If you select the **Non Recurring** radio button, specify the end date and time of daylight saving in the following fields: • **Year**. Configure the end year. • **Date**. Configure the end date. • **Month**. Configure the end month. • **Hours**. Configure the end hour. • **Minutes**. Configure the end minute.
Offset **Note:** These fields do not apply if you select the **Recurring** radio button or the **Non Recurring** radio button.	If you select the **Recurring EU** radio button or the **Recurring USA** radio button, you must specify the recurring offset of daylight saving time in minutes. This is the offset in relation to regular time, that is, when daylight saving time is not in effect. The default setting (offset) is 60 minutes.
Zone **Note:** These fields do not apply if you select the **Recurring** radio button or the **Non Recurring** radio button.	If you select the **Recurring EU** radio button or the **Recurring USA** radio button, you can specify the acronym associated with the time zone in which daylight saving is in effect. This field is not validated against any official list of time zone acronyms.

8. Click the **Apply** button.

   Your settings are saved.

View the DayLight Saving Time Status

You can view the status of daylight saving time (DST), including information about the daylight saving time settings and whether the time offset for daylight saving time is 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 *Access the Switch* on page 12.

   The login window opens.

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

The default password is **password**.

The System Information page displays.

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

   The DayLight Saving (DST) Status page displays.

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

The following table displays the nonconfigurable daylight saving status information.

Table 9. 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	Displays when the daylight saving time begins. This field is not displayed when daylight saving time is disabled.
Ends At	Displays when the daylight saving time ends. This field is not displayed when daylight saving time is disabled.
Offset (in Minutes)	The offset value in minutes.This field is not displayed when daylight saving time is disabled.
Zone	The zone acronym, if any was specified. This field is not displayed when daylight saving time is disabled.
Daylight Saving (DST) in Effect	Displays whether daylight saving time is in effect.

Configure DNS Settings

Use these pages to configure information about DNS servers that the network uses and how the switch operates as a DNS client.

Configure Global DNS Settings

Use the DNS Configuration page to configure global DNS settings and DNS server information.

➢ **To configure the global DNS settings:**

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

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

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

If you do not know the IP address of the switch, see *Access the Switch* on page 12.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The DNS Configuration page displays.

6. Select the **Disable** or **Enable** radio button to specify whether to disable or enable the administrative status of the DNS client:
   - **Enable**. Allow the switch to send DNS queries to a DNS server to resolve a DNS domain name. The DNS is enabled by default.
   - **Disable**. Prevent the switch from sending DNS queries.
7. In the **DNS Default Name** field, enter the default DNS domain name to include in DNS queries.

   When the system is performing a lookup on an unqualified host name, this field 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 158 characters.

8. To add a DSN server, do the following:
   a. In the **DNS Server** field in the DNS Server Configuration table, specify the IPv4 address to which the switch sends DNS queries.
   b. 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.

9. To remove a DNS server from the list, do the following:
   a. Select the check box for the server.
   b. Click the **Delete** button.
10. Click the **Apply** button.

    Your settings are saved.

11. To refresh the page, click the **Refresh** button.

The following table displays DNS Server Configuration information.

Table 10. DNS Server Configuration information

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

Configure and View Host Name-to-IP Address Information

Use this page to manually map host names to IP addresses or to 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 *Access the Switch* on page 12.

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

   The default password is **password**.

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

   The DNS Host Configuration page displays.
6. In the **Host Name (1 to 158 characters)** field, specify the static host name to add.

   Its length cannot exceed 158 characters and it is a required field.
7. In the **IPv4/IPv6 Address** field, enter the IP address to associate with the host name.
8. Click the **Add** button.

   The entry displays in the list on the page.

Remove an Entry From the Dynamic Host Mapping Table

➢ **To remove an entry from the dynamic host mapping table:**

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

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

   The default password is **password**.

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

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

   The entry is removed.

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

➢ **To change the host name or IP address in an entry of the dynamic host mapping table and view all entries:**

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

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

   The default password is **password**.

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

   The DNS Host Configuration page display.

6. Select the check box for 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 11. Dynamic Host Mapping information

Field	Description
Host	The host name that you assign to the specified IP address.
Type	The type of the dynamic entry.
IPv4/IPv6 Address	The IP address associated with the host name.

Configure Green Ethernet Settings

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

➢ **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 *Access the Switch* on page 12.

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

   The default password is **password**.

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

   The Green Ethernet Configuration page displays.

   Auto Power Down mode is enabled globally, but you can disable it on a per-port basis for ports g1–g4 (see *Manage and View the PoE Port Configuration* on page 55). You cannot disable it for other ports. If Auto Power Down mode is enabled on a port and the port link goes down, the physical layer (PHY) automatically shuts down for a short period and wakes up to check link pulses. This mode reduces power consumption on a port if no link partner is present.

Short Cable mode is enabled globally, but you can disable it on a per-port basis for ports g1–g4 (see *Manage and View the PoE Port Configuration* on page 55). You cannot disable it for other ports. If Short Cable mode is enabled on a port, and the cable length is too short, the PHY enters low-power mode.

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

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

7. Click the **Apply** button.

   Your settings are saved.

Configure Green Ethernet Interface Settings

Use this page to configure per-port Green Ethernet settings.

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

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The Green Ethernet Interface Configuration page displays.

6. Do one of the following:
   - In the **Go To Interface** field, enter the port using the respective naming convention (for example, g1 or g12), and click the **Go** button.

     The entry corresponding to the specified interface is selected.

     For more information about naming conventions, see *Interface Naming Conventions* on page 12.

- Select the port.

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

   The default is Disable, which is the global setting (see *Configure the Global PoE Settings* on page 53). For ports g1–g4 only, you can disable the mode.

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

   The default is Disable, which is the global setting (see *Configure the Global PoE Settings* on page 53). For ports g1–g4 only, you can disable the mode.

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

   The default is Disable. If the EEE mode is not supported, then N/A is displayed.

10. Click the **Apply** button.

    Your settings are saved.

Configure Green Ethernet Settings for Local Devices

Use this page to configure and view detailed per-port green Ethernet settings for local devices.

➢ **To configure and view green Ethernet for local devices:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The Local Device Information page displays.

6. From the **Interface** menu, select the interface.
7. To disable the Energy Detect Admin Mode for port g1, g2, g3, or g4, from the **Energy Detect Admin Mode**, select **Disable**.

   The Energy Detect Admin Mode is enabled globally, but you can disable it for ports g1–g4 only. With this mode enabled, the port transitions to low power mode during a link idle condition.

   The Operational Status field shows whether the energy detect operational status is active or inactive.

The Reason field shows the reason for the operational status.

8. To disable the Short Reach Admin mode for port g1, g2, g3, or g4, from the **Short Reach Admin mod**, select **Disable**.

   The Energy Detect Admin Mode is enabled globally, but you can disable it for ports g1–g4 only. With this mode enabled, the port transitions to low power mode when the cable length is too short.

   The Operational Status field shows whether the short reach operational status is active or inactive.

   The Reason field shows the reason for the operational status.

9. Use the **EEE Admin Mod**e menu to enable or disable this option on the port.

   With the EEE mode enabled, the port transitions to low power mode during a link idle condition. The default value is Disable.

10. Click the **Apply** button.

    Your settings are saved.

11. To refresh the page, click the **Refresh** button.
12. To clear the configuration, resetting all statistics for the selected interface to default values, click the **Clear** button.

The following table describes the nonconfigurable fields.

Table 12. Green Ethernet Local Device Information

Field	Description
Tw_sys_tx (uSec)	The value of Tw_sys that the local system can support.
Tw_sys_tx Echo (uSec)	The remote system's Transmit Tw_sys that was used by the local system to compute the Tw_sys that is requested from the remote system.
Tw_sys_rx (uSec)	The value of Tw_sys that the local system requests from the remote system.
Tw_sys_rx Echo (uSec)	The remote system's Receive Tw_sys that is used by the local system to compute the Tw_sys that it can support.

View Green Ethernet Information for Remote Devices

➢ **To view green Ethernet information for remote devices:**

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

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

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

If you do not know the IP address of the switch, see *Access the Switch* on page 12.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The Green Ethernet Details page displays.

6. Scroll down to the Remote Device Information section.
7. Form the **Interface** menu, select the interface.

The following table describes the nonconfigurable fields.

Table 13. Green Ethernet Remote Device Information

Field	Description
Remote ID	The remote client identifier assigned to the remote system.
Remote Tw_sys_tx (uSec)	The value of Tw_sys that the remote system can support.
Remote Tw_sys_tx Echo (uSec)	The value of Transmit Tw_sys echoed back by the remote system.
Remote Tw_sys_rx (uSec)	The value of Tw_sys that the remote system requests from the local system.
Remote Tw_sys_rx Echo (uSec)	The value of Receive Tw_sys echoed back by the remote system.

View the Green Ethernet Statistics Summary

This page summarizes the green Ethernet settings currently in use.

➢ **To view the green Ethernet statistics:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

The Green Mode Statistics Summary page displays. The page shows the Green Ethernet Interface Summary section.

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

The following table describes the nonconfigurable fields.

Table 14. Green Ethernet Statistics Summary information

Field	Description
Cumulative Energy Saving (Watts*Hours)	The estimated cumulative energy saved in watts * hours when all green modes are enabled.
Interface	The interface for which data is displayed or configured.
Energy Detect Admin mode	Shows whether Energy Detect mode is enabled or disabled on the port. If this mode is enabled and the port link goes down, the PHY automatically goes down for a short period of time, then wakes up to check link pulses. This allows the switch to perform autonegotiation and save power consumption when no link partner is present.
Energy Detect Operational Status	The current operational status of the Energy Detect mode.
Short Reach Admin mode	Shows whether Short Reach Admin mode is enabled or disabled on the port. When this mode is enabled, the PHY is forced to operate in low power mode irrespective of the cable length.
Short Reach Operational Status	The current operational status of the Short Reach mode.
EEE Admin mode	Shows whether Energy Efficient Ethernet mode is enabled or disabled on the port. When this mode is enabled, the port transitions to low power mode during link idle conditions.

Use the Device View

For information about the device view, see *Local Browser Interface Device View* on page 19.

Configure Power over Ethernet

Note: This section applies to model MS510TXPP only.

A Power over Ethernet (PoE) device is a type of power sourcing equipment (PSE) that delivers electrical power to connected powered devices (PDs) over existing Ethernet cables without interfering with the network traffic.

From the **System > PoE** menu, you can access pages that are described in the following sections:

- *PoE Overview* on page 51

- *Device Class Power Requirements* on page 51
- *Power Allocation and Power Budget* on page 52
- *Configure the Global PoE Settings* on page 53
- *Manage and View the PoE Port Configuration* on page 55

PoE Overview

Model MS510TXPP supports both IEEE 802.3af (PoE) and IEEE 802.3at (PoE+) on ports 1–8 with a maximum PoE power budget of 180W across all active PoE+ ports. You can globally specify the following:

- Limit port power based on the PD class or on user settings.
- Allow detection of both standards (802.3af and 802.3at)–based and legacy (pre-standard)–based PDs.
- Allow detection only of standard-based PDs.
- Enable or disable PoE related traps.

The power limit of a port is based on the global setting of the power limit type. If the power limit type is based on the PD class, the port limit is based on the class that is advertised by the PD attached to the port. If the power limit type is based on the user settings, the port limit is based on the maximum power limit that you configure for the port (the default is 30W).

On a per-port basis, you can enable or disable PoE and configure priority settings, timers, and power limits. Doing so allows you to manage the power supplied to the connected PDs and to ensure that the power budget is used effectively.

By default, supplied power is prioritized on the switch in ascending port order, up to the total power budget of the switch. If the power requirements for the attached PDs exceed the total power budget of the switch, the power to the device on the highest-numbered PoE+ port is disabled to make sure that the devices connected to the higher-priority, lower-numbered PoE+ ports are supported first.

Note: Although a device is listed as an 802.3at (PoE+) powered or 802.3af (PoE) powered device, it might not require the maximum power limit that is specified. Many devices require less power, allowing all eight PoE ports to be active simultaneously, when the devices correctly report their PoE class to the switch.

Device Class Power Requirements

PoE and PoE+ use Ethernet cables to supply power to PoE-capable devices on the network, such as WiFi access points, IP cameras, VoIP phones, and switches. The switch is compliant with the IEEE 802.3at standard (PoE+) and backward compatible with the IEEE 802.3af standard (PoE). The switch can pass power through to any powered device (PD) that

supports these standards. PoE and PoE+ let you power such devices without the need for a separate power supply.

The switch supports a Plug-and-Play process by which it detects the type of device that is connected to one of its PoE+ ports and whether that device needs power and how much so that the switch can provide the correct power the device.

During the Plug-and-Play process, the connected device can provide its Class response to the switch in many ways, depending on how the vendor programmed the device.

The following table shows the device classes for PoE+ devices adhering to the IEEE 802.3at standard. The device classes for PoE devices adhering to the IEEE 802.3af standard are identical with the exception that Device Class 4 is not supported.

Table 15. PoE and PoE+ device class power allocation

Device Class	Standard	Range of Power Delivered to the Powered Device	Minimum Output at PoE Switch Port (Minimum Allocated)	Maximum Output at PoE Switch Port (Maximum Allocated)
0	PoE and PoE+	0.44W–12.95W	15.4W	16.2W
1	PoE and PoE+	0.44W–3.84W	4.0W	4.2W
2	PoE and PoE+	3.84W–6.49W	7.0W	7.4W
3	PoE and PoE+	6.49W–12.95W	15.4W	16.2W
4	PoE+ only	12.95W–25.5W	30.0W	31.6W

Power Allocation and Power Budget

The switch is a smart switch in that it can allocate the required power to a connected device by using a prioritization scheme: By default, power is supplied in ascending port order (that is, lower port numbers are served first) until the power budget is consumed and insufficient power remains to allocate to the next device. When less than 7W of PoE power is available on a port, the port PoE LED lights yellow, and the attached device does not receive power from the port. However, the switch continues to send data through the port connection.

The switch is also a smart switch in that it can override the IEEE power classification of a powered device (PD): If the PD consumes less power than required by its power classification, the switch provides only the power that the PD consumes instead of the power that is required by the PD's power classification.

If some PoE+ ports are in use and deliver power, you can calculate the available power budget for the other PoE+ ports by subtracting the consumed (that is, delivered power) from the total available power budget. (For information about the total available power budget, see *PoE Overview* on page 51.)

An example:
Port 1 delivers 4.4W to a PD. The available power budget is 175.6W (180W–4.4W).

Another example:
A Class 4 PD is attached to Port 1, a Class 2 PD to Port 2, and another Class 4 PD to Port 3.

However, the PDs consume less power than defined by their classes: The PD attached to Port 1 consumes 7.3W, the PD attached to Port 2 consumes 4.7W, and the PD attached to Port 3 consumes 8.9W. So even though the switch provides power to two Class 4 devices and one Class 3 device, the available power budget is 159.1W (180W–7.3–4.7–8.9W).

➢ **To determine the delivered power by PoE+ 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 *Access the Switch* on page 12.

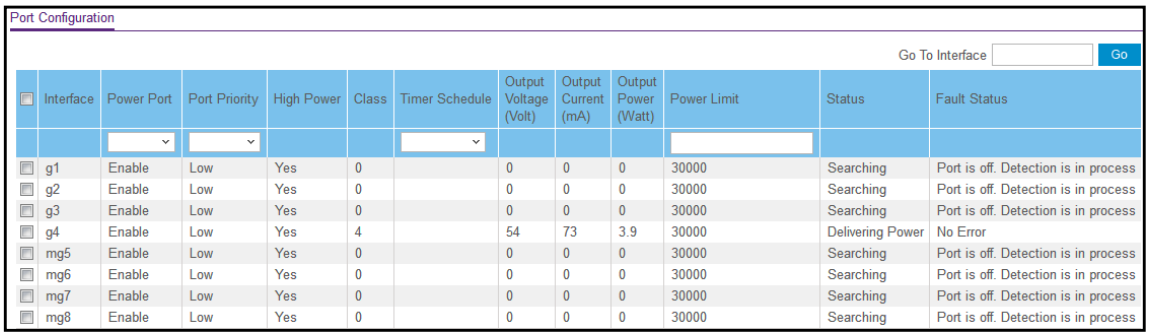
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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



   The delivered power is stated in the Output Power (Watt) column.

Configure the Global PoE Settings

➢ **To configure the global 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 *Access the Switch* on page 11.

   The login window opens.

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

   The default password is **password**. If you added the switch to a network on the Insight app before and you did not yet change the password through the local browser interface, enter your Insight network password.

   The System Information page displays.

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

   The PoE Configuration page displays.

6. Select one of the following Power Limit Type radio buttons:
   - **Class**. The maximum amount of power that can be delivered to a port is determined by the class of the attached PD.
   - **User**. The maximum amount of power that can be delivered to a port is determined by the power limit settings for the port (see *Manage and View the PoE Port Configuration* on page 55). This is the default setting.
7. Select one of the following Detection Type radio buttons:
   - **IEEE 802 + Legacy**. The ports support the IEEE 802.3at standard (PoE+), the IEEE 802.3af standard (PoE), and legacy PDs that require high-inrush current of more than 15W to power up. This is the default setting.
   - **IEEE 802**. The ports support the IEEE 802.3at standard (PoE+) and the IEEE 802.3af standard (PoE) but do not support legacy PDs.
8. Select one of the following Traps radio buttons:
   - **Disable**. No PoE traps are generated. This is the default setting.
   - **Enable**. PoE traps are generated if a PoE event occurs. PoE events could include events such as a port starting or stopping providing PoE power or the switch reaching a threshold power level.
9. Click the **Apply** button.

   Your setting are saved.

The following table describes the nonconfigurable fields on the page.

Table 16. PoE Configuration fields

Field	Description
Power Status	The power status.
Nominal Power	The maximum amount of power in watts that the switch can deliver to all ports.
Threshold Power	If the consumed power is below the threshold power, the switch can power up another port. The consumed power can be between the nominal and threshold power. The threshold power is displayed in watts.
Consumed Power	The total amount of power in watts that is being delivered to all ports.

Manage and View the PoE Port Configuration

Depending on the model, the switch includes eight PoE+ ports.

➢ **To configure and view 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 *Access the Switch* on page 12.

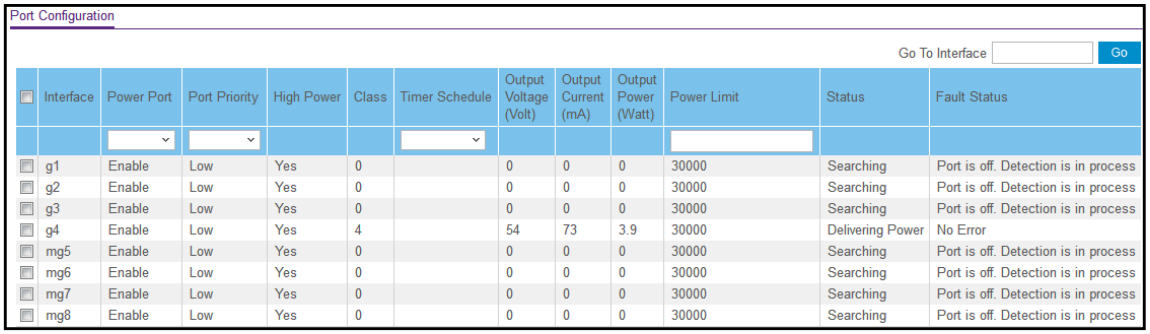
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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



Interface	Power Port	Port Priority	High Power	Class	Timer Schedule	Output Voltage (Volt)	Output Current (mA)	Output Power (Watt)	Power Limit	Status	Fault Status
g1	Enable	Low	Yes	0		0	0	0	30000	Searching	Port is off. Detection is in process
g2	Enable	Low	Yes	0		0	0	0	30000	Searching	Port is off. Detection is in process
g3	Enable	Low	Yes	0		0	0	0	30000	Searching	Port is off. Detection is in process
g4	Enable	Low	Yes	4		54	73	3.9	30000	Delivering Power	No Error
mg5	Enable	Low	Yes	0		0	0	0	30000	Searching	Port is off. Detection is in process
mg6	Enable	Low	Yes	0		0	0	0	30000	Searching	Port is off. Detection is in process
mg7	Enable	Low	Yes	0		0	0	0	30000	Searching	Port is off. Detection is in process
mg8	Enable	Low	Yes	0		0	0	0	30000	Searching	Port is off. Detection is in process

6. In the Interface column, select the check boxes for the PoE+ ports that you want to configure or select the check box in the heading to configure the same settings for all eight PoE+ ports.
7. Configure the settings as described in the following table.

The settings that you configure apply to all selected PoE+ ports.

Menu Item	Description
Port Power	Select the administrative 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.
Port Priority	The port priority determines which ports can still deliver power after the total power delivered by the switch exceeds the total power budget of 180W. (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. Select one of the following priorities: • **Low**. Low priority. This is the default setting. • **Medium**. Medium priority. • **High**. High priority.
Timer Schedule	If you set up a PoE timer schedule, you can assign it to the port by selecting the schedule from the **Timer Schedule** menu. For information about PoE timer schedules, see *Set Up PoE Timer Schedules* on page 80. By default, the selection from the menu is None. If you want to remove a previously assigned timer schedule, select **None** from the **Timer Schedule** menu.
Power Limit (W)	Enter the maximum power milliwatt (mW) that the port can deliver. The maximum and default power is 30,000 mW.

8. Click the **Apply** button.

   Your settings are saved.

   The following table describes the nonconfigurable fields on the PoE Port Configuration page.

Field	Description
High Power	If a port supports High Power mode, the field displays Yes.
Class	The class defines the range of power 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
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 (W)	The power that is delivered to the PD in watts.

Field	Description
Status	The operational status of the port. The possible values are as follows: • **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. • **Test**. The port is in test mode. • **Other Fault**. The port is idle because of an error condition. • **Searching**. The port is not in one of the other states in this list.
Fault Status	The description when the PoE port is in a fault or non-errors state. The possible values are as follows: • **Port is off. Detection is in process**. The port is not delivering power but can detect whether a PD is being attached to the port. • **No Error**. The port is not in any error state and provides power. The fault status can also be any of the following: • **Main supply high voltage**. • **Main supply low voltage**. • **Hardware pin disabled**. • **Non 802-3af powered device**. • **Overload**. • **Underload**. • **Overload and underload**. • **Budget exceeded**. • **Voltage injection**. • **Improper capacitor detection**. • **Discharged load**. • **Forced power – overload**. • **Short**. • **Port overheat**. • **Device overheat**. • **Class error**.

Configure SNMP

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

The switch uses both standard public MIBs for standard functionality and private MIBs that support additional switch functionality. 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.

From the **System > SNMP** menu, you can access pages that are described in the following sections:

- *Configure the SNMPv1/v2 Community* on page 58
- *Configure SNMPv1/v2 Trap Settings* on page 60
- *Configure SNMPv1/v2 Trap Flags* on page 62
- *View the Supported MIBs* on page 63
- *Configure SNMPv3 Users* on page 64

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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > SNMP > SNMPv1/v2 > Community Configuration**.

   The Community Configuration page displays.

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

   Together, the management station IP and the management station IP mask denote a range of IP addresses from which SNMP clients can use that community to access this device. If either the management station IP or management station IP mask value is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's address is ANDed with the mask, as is the management station IP address. If the values are equal, access is allowed. For example, if the management station IP and management station IP mask parameters are 192.168.1.0/255.255.255.0, then any client whose address is

192.168.1.0 through 192.168.1.255 (inclusive) is allowed access. To allow access from only one station, use a management station IP mask value of 255.255.255.255, and use that machine's IP address for client address.

8. In the **Community String** field, specify a community name.
9. From the **Access Mode** menu, select the access level for this community, which is either **Read/Write** or **Read Only**.
10. From the **Status** menu, select to enable or disable the community.

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

11. Click the **Add** button.

    The selected community is added.

Modify an Existing SNMP Community

➢ **To modify an existing SNMP community:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > SNMP > SNMPv1/v2 > Community Configuration**.

   The Community Configuration page displays.

6. Select the check box for 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > SNMP > SNMPv1/v2 > Community Configuration**.

   The Community Configuration page displays.

6. Select the check box for 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

The System Information page displays.

5. Select **System > SNMP > SNMPv1/v2 > Trap Configuration**.

   The Trap Configuration page displays.

6. In the **Recipients IP** field, enter the IPv4 address in the x.x.x.x format to receive SNMP traps from this device.
7. From the **Version** menu, select the trap version to be used by the SNMP trap receiver:
   - **SNMPv1**. The switch uses SNMPv1 to send traps to the receiver.
   - **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. 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > SNMP > SNMPv1/v2 > Trap Configuration**.

   The Trap Configuration page displays.

6. Select the check box for the recipient.
7. Update the fields as needed.
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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > SNMP > SNMPv1/v2 > Trap Configuration**.

   The Trap Configuration page displays.

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

   The trap recipient is removed.

Configure SNMPv1/v2 Trap Flags

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

➢ **To 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > SNMP > SNMPv1/v2 > Trap Flags**.

   The Trap Flags page displays.

6. Configure the following options:
   - **All**. Globally activate or disable all traps by selecting the corresponding radio button. By default, the Enable radio button is selected.
   - **Authentication**. When authentication is enabled, SNMP traps are sent when events involving authentication occur. By default, the Enable radio button is selected.
7. Click the **Apply** button.

   Your settings are saved.

View the Supported MIBs

This page displays a list of all MIBs supported by the switch.

➢ **To view the supported MIBs:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > SNMP > SNMPv1/v2 > Supported MIBs**.

   The Status page displays.

The following table describes the fields on the Status page.

Table 17. 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 SNMPv3 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **System > SNMP > SNMPv3 > User Configuration**.

   The User Configuration page displays.

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

6. To enable authentication, select an Authentication Protocol radio button.

   You can select the **MD5** radio button or the **SHA** radio button. With either of these options, the user login password is used as SNMPv3 authentication password. For information about how to configure the login password, see *Change the Password* on page 216.

7. To enable encryption, do the following:
   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. This information is viewed by a network manager to identify system topology and detect bad configurations on the LAN.

From the **System > LLDP > Advanced** menu, you can access pages that are described in the following sections:

- *Configure LLDP Global Settings* on page 65
- *Configure LLDP Port Settings* on page 67
- *LLDP-MED Network Policy* on page 68
- *LLDP-MED Port Settings* on page 69
- *Local Information* on page 70
- *Neighbors Information* on page 72

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

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

➢ **To configure global LLDP settings:**

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

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

2. Launch a web browser.

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The LLDP Properties page displays. The page also displays the LLDP-MED Properties section.

6. To configure nondefault values for the following LLDP properties, specify the following options:
   - **LLDP Status**. Enable or disable the LLDP feature.
   - **Forward LLDP PDUs while LLDP Disabled**. Enable or disable this feature.

     If you select the **Enable** radio button for this feature but the LLDP Status **Disable** radio button is selected, LLDP PDUs are flooded to all ports. By default, this setting is disabled, which means that LLDP PDUs are dropped if the LLDP Status **Disable** radio button is selected.

   - **TLV Advertised Interval**. The number of seconds between transmissions of LLDP advertisements.
   - **Hold Multiplier**. The transmit interval multiplier value, where transmit hold multiplier x 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

Use the LLDP Port Settings page to 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The LLDP Port Settings page displays.

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. 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.
     - **Disable**. Do not transmit or receive LLDP PDUs on the selected ports.

     The default is Tx and Rx.

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

The default is Auto Advertise.

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

  For information about how to configure the system name, see *View and Configure the Switch Management Settings* on page 24. For information about how to configure the port description, see *Configure the Port Settings* on page 88.

8. Click the **Apply** button.

   Your settings are saved.

LLDP-MED Network Policy

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

➢ **To 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The LLDP-MED Network Policy page displays.

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

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

   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 18. LLDP-MED network policy information

Field	Description
Network Policy Number	The policy number.
Application	The media application type that is associated with the policy. Only the voice application type is supported. The application type that is received on the interface includes the VLAN ID, priority, DSCP, tagged bit status, and unknown bit status. 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.

LLDP-MED Port Settings

Use this page to 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 *Access the Switch* on page 12.

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

   The default password is **password**.

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

   The LLDP-MED Port Settings page displays.
6. From the **Port** menu, select the port to configure.

7. Use the following menus to enable or disable the following LLDP-MED settings for the selected port:
   - **LLDP-MED Status**. The administrative status of LLDP-MED on the interface. When LLDP-MED is enabled, the transmit and receive function of LLDP is effectively enabled on the interface.
   - **Notification**. When enabled, the port sends a topology change notification if a device is connected or removed.
   - **Transmit Optional TLVs**. When enabled, the port transmits the following optional TLVs in the LLDP PDU frames:
     - MED Capabilities
     - Location Identification
     - Extended Power via MDI: PSE
     - Extended Power via MDI: PD
     - Inventory
8. Click the **Apply** button.

   Your settings are saved.

Local Information

Use the LLDP Local Information page to 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 *Access the Switch* 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 > Advanced > LLDP > Local Information**.

   The Device Information page displays. The page also displays the Port Information section.

   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.
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.
Interface	The interface associated with the rest of the data in the row.
LLDP Local Information	
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* on page 88.
Advertisement	The TLV advertisement status of the port.

6. To view additional details about a port, click the port (which is a hyperlink) in the Interface column of the Port Information table.

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

Field	Description
Managed Address	
Address SubType	The type of address the management interface uses, such as an IPv4 address.
Address	The address used to manage the device.
Interface SubType	The port subtype.
Interface Number	The number that identifies the port.
MAC/PHY Details	
Auto Negotiation Supported	Indicates whether the interface supports port speed autonegotiation. The possible values are True and False.
Auto Negotiation Enabled	The port speed autonegotiation support status. The possible values are True (enabled) or False (disabled).
Auto Negotiation Advertised Capabilities	The port speed autonegotiation capabilities such as 1000BASE-T half-duplex mode or 100BASE-TX full-duplex mode.

Field	Description
Operational MAU Type	The Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interface collision detection and bit injection into the network.
MED Details	
Capabilities Supported	The MED capabilities enabled on the port.
Current Capabilities	The TLVs advertised by the port.
Device Class	Network Connectivity indicates that the device is a network connectivity device.
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.

Neighbors Information

Use the LLDP Neighbors Information page to 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 *Access the Switch* 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 > Advanced > LLDP > Neighbor 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 hyperlink in the MSAP Entry column.

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

   The following table describes the information transmitted by the neighbor.

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

Field	Description
Managed Addresses	
Address SubType	The type of the management address.
Address	The advertised management address of the remote system.
Interface SubType	The port subtype.
Interface Number	The port on the remote device that sent the information.
MAC/PHY Details	
Auto-Negotiation Supported	Specifies whether the remote device supports port-speed autonegotiation. The possible values are True or False.
Auto-Negotiation Enabled	The port speed autonegotiation support status. The possible values are True and False.
Auto Negotiation Advertised Capabilities	The port speed autonegotiation capabilities.
Operational MAU Type	The Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interface collision detection and bit injection into the network.
MED Details	
Capabilities Supported	The supported capabilities that were received in MED TLV from the device.
Current Capabilities	The advertised capabilities that were received in MED TLV from the device.
Device Class	The LLDP-MED endpoint device class. The possible device classes are as follows: • 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 type of PoE for the port, for example, powered.
PoE Power Source	The power source for the port.
PoE Power Priority	The power priority for the port.
PoE Power Value	The power value for the port.
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
Manufacturer Name	The manufacturer name advertised by the remote device.
Model Name	The model name advertised by the remote device.
Asset ID	The asset ID advertised by the remote device.
Location Information	
Civic	The physical location, such as the street address, that the remote device advertised in the location TLV, for example, 123 45th St. E. The field value length range is 6–160 characters.
Coordinates	The location map coordinates that the remote device advertised in the location TLV, including latitude, longitude, and altitude.
ECS ELIN	The Emergency Call Service (ECS) Emergency Location Identification Number (ELIN) that the remote device advertised in the location TLV. The field range is 10–25.
Unknown	Displays unknown location information for the remote device.
Network Policies	
Application Type	The media application type associated with the policy advertised by the remote device.
VLAN ID	The VLAN ID associated with the policy.
VLAN Type	Specifies whether the VLAN associated with the policy is tagged or untagged.
User Priority	The priority associated with the policy.
DSCP	The DSCP associated with a particular policy type.
LLDP Unknown TLVs	
Type	The unknown TLV type field.
Value	The unknown TLV value field.

Configure DHCP Snooping

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

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

From the **System > Services** menu, you can access pages that are described in the following sections:

- *Configure the Global DHCP Snooping Settings* on page 76
- *Enable DHCP for All Interfaces in a VLAN* on page 77
- *Configure DHCP Snooping Interface Settings* on page 77
- *Configure Static DHCP Bindings* on page 78
- *Configure the DHCP Snooping Persistent Settings* on page 80

Configure the Global DHCP Snooping Settings

Use this page to 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 *Access the Switch* on page 12.

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

   The default password is **password**.

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

   The DHCP Snooping Global Configuration page displays.
6. Select the DHCP Snooping Mode **Enable** radio button.
7. To enable the verification of the sender's MAC address for DHCP snooping, select the MAC Address Validation **Enable** radio button.

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

   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 *Access the Switch* on page 12.

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

   The default password is **password**.

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

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

   Your settings are saved.

Configure DHCP Snooping Interface Settings

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

➢ **To 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 *Access the Switch* on page 12.

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

   The default password is **password**.

The System Information page displays.

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

   The DHCP Snooping Interface Configuration page displays.

6. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
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 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.
8. From the **Trust Mode** menu, select the desired trust mode:
   - **Disabled**. The interface is considered to be untrusted and could potentially be used to launch a network attack. DHCP server messages are checked against the bindings database. On untrusted ports, DHCP snooping enforces the following security rules:
     - DHCP packets from a DHCP server (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.
9. Click the **Apply** button.

   Your settings are saved.

Configure Static DHCP Bindings

Use this page to 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The Static Binding Configuration page displays. The page also shows the Dynamic Binding Configuration section.

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

   This is the key to the binding database.

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

    The DHCP snooping binding entry is added to the database.

The Dynamic Binding Configuration table shows information about the DHCP bindings that were learned on each interface on which DHCP snooping is enabled.

The following table describes the dynamic bindings information.

Table 19. 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 the 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.

➢ **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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The DHCP Snooping Persistent Configuration page displays.

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

   The binding table is stored locally on the switch. By default, the **Disable** radio button is selected.

7. Click the **Apply** button.

   Your settings are saved.

Set Up PoE Timer Schedules

Note: This section applies to model MS510TXPP only.

The switch lets you define multiple timer schedules that you can use for PoE power delivery to attached powered devices (PDs).

After you create a timer schedule, you can associate it with one or more PoE ports (see *Manage and View the PoE Port Configuration* on page 55). 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. That is, when a timer schedule is active, PoE is disabled on the port. When the timer schedule is inactive, PoE is enabled on the port.

Note: Timer schedules can function only if the switch clock was set, either manually or by SNTP (see *Configure the Time Settings* on page 32). If the switch clock is set to the default clock, timer schedules do not take effect.

You can create absolute schedules, which apply to specific dates and times, and you can create recurring schedules.

From the **System > Timer Schedule** menu, you can access pages that are described in the following sections:

- *Create a PoE Timer Schedule* on page 81
- *Specify the Settings for a PoE Timer Schedule* on page 82
- *Add a Periodic Schedule for a PoE Timer Schedule* on page 83
- *Delete a Periodic Schedule for a PoE Timer Schedule* on page 84
- *Delete a PoE Timer Schedule* on page 85

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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The Timer Schedule Name page displays.

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

   The timer schedule is added to the table on the Timer Schedule Name page.

Specify the Settings for a PoE Timer Schedule

A PoE timer schedule can start either immediately or at a specific time on a specific date. Similarly, a PoE timer schedule can continue indefinitely (or until you change the settings) or end at a specific time on a specific date.

For each PoE timer schedule, you can add multiple periodic schedules that are repeated every week while the PoE timer schedule is active (see *Add a Periodic Schedule for a PoE Timer Schedule* on page 83) and that complement the PoE timer schedule.

➢ **To specify the settings for a PoE timer schedule:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The Timer Schedule Configuration page displays.

6. From the **Timer Schedule Name** menu, select the name of the timer schedule for which you want to add a periodic schedule.

   You can select only names of schedules that you created (see *Create a PoE Timer Schedule* on page 81).

7. Click the **Add** button.

   If you select the **Immediate** radio button, the timer schedule is enabled immediately after you complete the configuration for the timer schedule. You do not need to specify the date and time that the timer schedule starts.

   If you select the **Specific** radio button, specify the date and time that the timer schedule starts by doing the following:

   a. Click in the **Timer Schedule Absolute Start Date** field to display a calendar and select the start date from the calendar.
   b. In the **Timer Schedule Absolute Start Time** field, enter the start time in the hh:mm 24-hour format.

8. Select the Timer Schedule Absolute End **Permanent** or **Specific** radio button.

If you select the **Permanent** radio button, the timer schedule continues indefinitely (or until you change the settings) after you complete the configuration for the timer schedule. You do not need to specify the date and time that the timer schedule ends.

If you select the **Specific** radio button, specify the date and time that the timer schedule ends by doing the following:

a. Click in the **Timer Schedule Absolute End Date** field to display a calendar and select the end date from the calendar.

b. In the **Timer Schedule Absolute End Time** field, enter the end time in the hh:mm 24-hour format.

9. Click the **Apply** button.

   Your settings are saved.

   For information about associating the PoE timer schedule with one or more PoE ports, see *Manage and View the PoE Port Configuration* on page 55.

Add a Periodic Schedule for a PoE Timer Schedule

For each PoE timer schedule, you can add multiple periodic schedules that are repeated every week while the PoE timer schedule is active. For each entry, you can specify the days of the week and the start and end time that applies to all selected days.

A periodic timer schedule complements the PoE timer schedule. If you do not add a periodic timer schedule, the PoE timer schedule is active continuously after you enable it.

➢ **To add a periodic schedule for a PoE timer schedule:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The Timer Schedule Configuration page displays.

6. From the **Timer Schedule Name** menu, select the 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 81).

7. Select the check boxes for the days on which the PoE timer schedule must be active.
8. In the **Start Time** field, enter the start time in the hh:mm 24-hour format.

   The start time applies to all selected days.
9. In the **End Time** field, enter the end time in the hh:mm 24-hour format.

   The end time applies to all selected days.
10. Click the **Apply** button.

    Your settings are saved.
11. Select **System > Timer Schedule > Advanced > Timer Schedule Configuration**.

    The Timer Schedule Configuration page displays. The timer schedule that you just added displays in the Periodic Schedule Table.

Delete a Periodic Schedule for a PoE Timer Schedule

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

➢ **To delete a periodic schedule for a PoE timer schedule:**

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

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

   The default password is **password**.

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

   The Timer Schedule Configuration page displays.
6. In the Periodic Schedule Table, select the check box for the periodic schedule that you want to delete.
7. Click the **Delete** button.

   The period schedule is deleted.

Delete a PoE Timer Schedule

You can delete a PoE timer schedule that you no longer need. All periodic schedules 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The Timer Schedule Name page displays.

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

   The schedule is deleted.

Configure Switching

3

This chapter covers the following topics:

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

Configure Port Settings and Flow Control

You can configure global flow control for all ports and view, configure, and monitor the port information for individual ports.

From the **Switching > Ports** menu, you can access pages that are described in the following sections:

- *Configure IEEE 802.3x Global Flow Control* on page 87
- *Configure the Port Settings* on page 88

Configure IEEE 802.3x Global Flow Control

Flow control helps to prevent data loss when the port cannot keep up with the number of frames being switched. When flow control is enabled, the switch can send a pause frame to stop traffic on a port if the amount of memory used by the packets on the port exceeds a preconfigured threshold and responds to pause requests from partner devices.

The paused port does not forward packets for the period of time specified in the pause frame. When the pause frame time elapses, or the utilization returns to a specified low threshold, the switch enables the port to again transmit frames.

➢ **To configure port settings:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Ports > Global Configuration**.

   The Global Configuration page displays.

6. Next to Global Flow Control (IEEE 802.3x) Mode, enable or disable IEEE 802.3x flow control on the system:
   - **Enable**. The switch sends pause packets if the port buffers become full. That is, flow control is enabled.
   - **Disable**. The switch does not send pause packets if the port buffers become full. That is, flow control is disabled. This the default setting.

7. Click the **Apply** button.

   Your settings are saved.

Configure the Port Settings

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

➢ **To configure port settings:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Ports > Port Configuration**.

   The Port Configuration pager displays.

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

   The description can be up to 64 characters in length.

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

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

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

   The supported speeds depends on the interface:

   - **Ports g1-g4**. Support the setting of 10 Mbps half duplex, 10 Mbps full duplex, 100 Mbps half duplex, 100 Mbps full duplex (FD), and Auto. When set to Auto, the port advertises 10/100 Mbps half and full duplex and 1000 Mbps full duplex.

- **Ports mg5-mg6**. Support the setting of 100 Mbps FD, 1 Gbps FD, and Auto. When set to Auto, the port advertises 100 Mbps FD, 1000 Mbps FD, and 2.5 Gbps FD.
- **Ports mg7-mg8**. Support the setting of 100 Mbps full duplex, 1Gbps FD, 2.5Gbps FD, and Auto. When set to Auto, the port advertises 100 Mbps FD, 1 Gbps FD, 2.5 Gbps FD, and 5 Gbps FD.
- **Port xmg9**. Supports the setting of 100 Mbps FD, 1 Gbps FD, 2.5 Gbps FD, 5 Gbps FD, and Auto. When set to Auto, the port advertises 100 Mbps FD, 1 Gbps FD, 2.5 Gbps FD, 5 Gbps FD, and 10 Gbps FD.
- **Port xg10**. Supports the setting of 1 Gbps FD and Auto.

Note: If you select multiple ports, the available options are determined by the common capabilities for the selected interfaces.

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

10. 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 possible values are as follows: • **Mirrored**. The port is a mirrored port on which all the traffic is copied to the probe port. • **Probe**. Use this port to monitor a mirrored port. • **LAG**. The port is a member of a link aggregation trunk. For more information, see *Configure Link Aggregation Groups* on page 89.
Physical Status	The port speed and duplex mode.
Link Status	Indicates whether the link is up or down. If the link is down because of a of switch action rather than the configured settings or a physical status, a reason is also provided.
MAC Address	The physical address of the specified interface.
ifIndex	The ifIndex of the interface table entry associated with this port.

Configure Link Aggregation Groups

Link aggregation groups (LAGs), which are also known as port channels, allow you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. You assign the LAG VLAN membership after you create a LAG. The LAG by default becomes a member of the default management VLAN (that is, VLAN 1).

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

Static LAGs are supported. When a port is added to a LAG as a static member, it neither transmits nor receives LACPDUs. The switch supports 8 LAGs.

From the **Switching > LAG > Advanced** menu, you can access pages that are described in the following sections:

- *Configure LAG Settings* on page 90
- *Configure LAG Membership* on page 92
- *Set the LACP System Priority* on page 93
- *Set the LACP Port Priority Settings* on page 93

Configure LAG Settings

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

Only interfaces of the same type as the other interfaces in the LAG can be added to a LAG. Therefore, only the following port groups can be members in the same LAG: g1 to g4 (a 1G LAG) or ports mg5 to mg6 (2.5G LAG), or ports mg5 to mg6 (5G LAG) or ports xmg9 and xg10 (10G LAG).

➢ **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 *Access the Switch* on page 12.

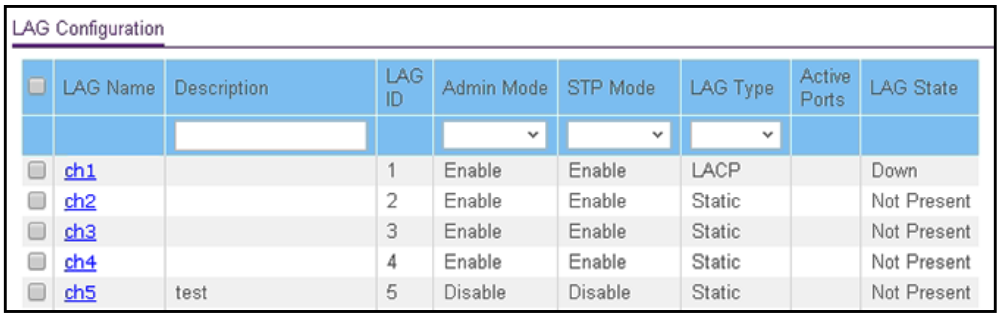
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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



LAG Configuration

	LAG Name	Description	LAG ID	Admin Mode	STP Mode	LAG Type	Active Ports	LAG State
	ch1		1	Enable	Enable	LACP		Down
	ch2		2	Enable	Enable	Static		Not Present
	ch3		3	Enable	Enable	Static		Not Present
	ch4		4	Enable	Enable	Static		Not Present
	ch5	test	5	Disable	Disable	Static		Not Present

6. Select one or more LAGs by taking one of the following actions:
   - To configure a single LAG, select the check box associated with the LAG.
   - To configure multiple LAGs with the same settings, select the check box associated with each LAG.
   - To configure all LAGs with the same settings, select the check box in the heading row.
7. In the **LAG Name** field, enter the name to be assigned to the LAG.

   You can enter any string of up to 15 alphanumeric characters. A valid name must be specified for you to create the LAG.
8. In the **Description** field, enter the description string to be attached to a LAG.

   The description can be up to 64 characters in length.
9. 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.
10. From the **STP Mode** menu, select the Spanning Tree Protocol (STP) administrative mode associated with the LAG. The possible values are as follows:
    - **Disable**. Spanning tree is disabled for this LAG.
    - **Enable**. Spanning tree is enabled for this LAG. Enable is the default.
11. From the **LAG Type** menu, select **Static** or **LACP**:
    - **Static**. Disables Link Aggregation Control Protocol (LACP) on the selected LAG. The LAG is configured manually. The default is Static.

      A static LAG does not transmit LACP PDUs or process incoming LACP PDUs. That is, the member ports of a LAG do not transmit LACP PDUs and all incoming LACP PDUs are dropped.
    - **LACP**. Disables LACP on the selected LA. The LAG is configured automatically.

    Note: You can change the LAG type only if the LAG includes members and the LAG is up.
12. 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.

Interfaces that you add to a LAG must be of the same type. Therefore, only the following port groups can be members in the same LAG: g1–g4 for a 1G LAG), ports mg5 and mg6 for either a 2.5G LAG or a 5G LAG, and ports xmg9 and xg9 for a 10G LAG.

➢ **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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The LAG Membership page displays.

6. From the **LAG ID** menu, select the LAG ID.

   The LAG Name field shows the name that is assigned to the LAG. You cannot change this name. The names are ch1, ch2, and so on through ch8.

7. To display the ports that are members of a LAG, click the **Current members** button.

   A pop-up window opens and shows the ports that are members of the LAG, if any.

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

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

➢ **To configure LACP:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > LAG > Advanced > LACP Configuration**.

   The LACP Configuration page displays.

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

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

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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > LAG > Advanced > LACP Port Configuration**.

   The LACP Port Configuration page displays.

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

7. In the **LACP Priority** field, specify the LACP priority value for the selected interfaces.

   This value specifies the device's link aggregation priority relative to the devices at the other ends of the links on which link aggregation is enabled. A higher value indicates a lower priority. The range is 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 given port can handle traffic for more than one VLAN, but it can support only one default VLAN ID.

You can define VLAN groups that are placed in the VLAN membership table. The switch supports up to 256 VLANs (with a VLAN ID from 1–4093). VLAN 1 is the default VLAN of which all ports are members.

From the **Switching > VLAN > Advanced** menu, you can access pages that are described in the following sections:

- *Configure VLAN Settings* on page 95
- *Configure VLAN Membership* on page 97
- *View VLAN Status* on page 99
- *Configure Port PVID Settings* on page 100
- *Configure MAC-Based VLAN Groups* on page 102
- *Manually Add Members to or Remove Them From a MAC-Based VLAN Group* on page 104
- *Configure Protocol-Based VLAN Groups* on page 104
- *Manually Add Members to or Remove Them From a Protocol-Based VLAN Group* on page 106
- *Configure GARP Switch Settings* on page 107
- *Configure GARP Ports* on page 108

Configure 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The VLAN Configuration page displays. The page also shows the Reset section.

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

   The range of the VLAN ID can be from 2 to 4093. VLAN ID 1 is reserved for the default VLAN.

7. In the **VLAN Name** field, specify a name for the VLAN.

   The VLAN name can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always uses the name Default.

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

   You cannot change the type of the default VLAN (VLAN ID = 1): it is always type Default. When you create a VLAN using this page, its type is always Static. A VLAN that is created by GVRP registration initially uses a type of Dynamic. When configuring a dynamic VLAN, you can change its type to Static.

9. Click the **Add** button.

   The VLAN is added to the switch.

10. Click the **Apply** button.

    Your settings are saved.

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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The VLAN Configuration page displays.

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

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

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

---

7. Click the **Delete** button.

   The VLAN is removed.

Reset All VLANs to the Default Settings

➢ **To reset all VLANs 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > VLAN > Advanced > VLAN Configuration**.

   The VLAN Configuration page displays.

6. Select the **Reset Configuration** check box.
7. Click the **Apply** button.

   Your settings are saved.

   The default values are as follows:

   - All ports are assigned to default VLAN 1.
   - All ports are configured with PVID 1.

   All VLANs, except for the default VLAN, are deleted.

Configure VLAN Membership

➢ **To configure VLAN membership:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

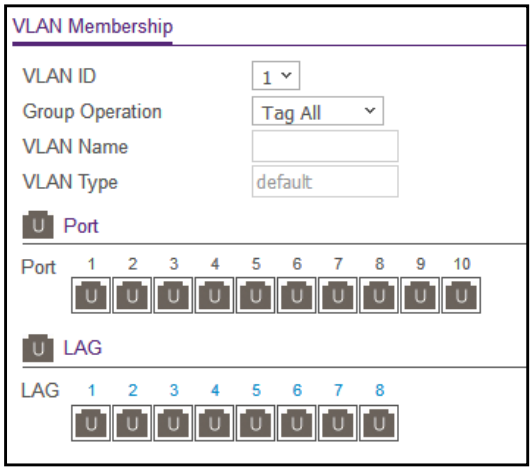
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > VLAN > Advanced > VLAN Membership**.



6. In the **VLAN ID** menu, select the VLAN ID.
7. In the **Group Operation** menu, select one of the following options, which applies to all ports in the VLAN:
   - **Tag All**. For all ports that are members of the VLAN, all egress packets are tagged.
   - **Untag All**. For all ports that are members of the VLAN, tags are removed from all egress packets.
   - **Remove All**. All ports that were dynamically registered through GVRP are removed from the VLAN.
8. In the Ports table, click each port once, twice, or three times to configure one of the following modes or reset the port to the default settings:
   - **T (Tagged)**. Select the ports on which all frames transmitted for this VLAN are tagged. The ports that are selected are included in the VLAN.
   - **U (Untagged)**. Select the ports on which all frames transmitted for this VLAN are untagged. The ports that are selected are included in the VLAN.

   By default, the selection is blank, which means that the port is excluded from the VLAN but can be dynamically registered (autodetected) in the VLAN through GVRP.
9. In the LAG table, click each LAG once, twice, or three times to configure one of the following modes or reset the LAG to the default settings:
   - **T (Tagged)**. Select the LAGs on which all frames transmitted for this VLAN are tagged. The LAGs that are selected are included in the VLAN.
   - **U (Untagged)**. Select the LAGs on which all frames transmitted for this VLAN are untagged. The LAGs that are selected are included in the VLAN.

   By default, the selection is blank, which means that the LAG is excluded from the VLAN but can be dynamically registered (autodetected) in the VLAN through GVRP.

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. VLAN ID 1 always uses the name Default.
VLAN Type	The type of the VLAN you selected: • **Default**. The management VLAN is created automatically. By default, this is VLAN 1. • **Static**. A VLAN that you configured. • **Dynamic**. A VLAN created by GVRP registration that you did not convert to static, and that GVRP can therefore remove.

View VLAN Status

You can view the status of all currently configured VLANs.

➢ **To view the VLAN status:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The VLAN Status page displays.

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 1 to 4093.
VLAN Name	The name of the VLAN. VLAN ID 1 is always named Default.
VLAN Type	The VLAN type: • **Default** (VLAN ID = 1). Always present. • **Static**. A VLAN that you configured. • **Dynamic**. A VLAN created by GVRP registration that you did not convert to static, and that GVRP can therefore remove.
Routing Interface	The interface associated with the VLAN, in the case that VLAN routing is configured for this VLAN.
Member Ports	The ports and LAGs that are included in the VLAN.

Configure Port PVID Settings

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

- You must define a PVID for all ports.
- If no other value is specified, the default VLAN PVID is used.
- To change the port's default PVID, you must first create a VLAN that includes the port as a member.
- Use the Port VLAN ID (PVID) Configuration page to configure a virtual LAN on a port.

➢ **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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

The Port PVID Configuration page displays.

6. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
7. Do one of the following:
   - 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.
8. In the **PVID** field, specify the VLAN ID to assign to untagged or priority-tagged frames received on this port.

   The default is 1.
9. In the **VLAN Member** field, specify the VLAN ID or list of VLANs of a member port.

   VLAN IDs range from 1 to 4093. The default is 1. Use a hyphen (-) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.
10. In the **VLAN Tag** field, specify the VLAN ID or list of VLANs of a tagged port.

    VLAN IDs range from 1 to 4093. Use a hyphen (-) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted. To reset the VLAN tag configuration to the defaults, select **None**. Port tagging for the VLAN can be set only if the port is a member of this VLAN.
11. From the **Acceptable Frame** menu, specify the types of frames that can be received on this port.

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

    - **VLAN only**. Untagged frames or priority-tagged frames received on this port are discarded.
    - **Admit All**. Untagged frames or priority-tagged frames received on this port are accepted and assigned the value of the port VLAN ID for this port. With either option, VLAN-tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
12. From the **Ingress Filtering** menu, select one of the following options:
    - **Enable**. The frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the port VLAN ID specified for the port that received this frame. The default is Enable.
    - **Disable**. All frames are forwarded in accordance with the 802.1Q VLAN bridge specification.
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.

Configure MAC-Based VLAN Groups

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 the desired VLAN ID. The MAC-to-VLAN configurations are shared across all ports of the device (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 the user is allowed to configure a MAC address mapping to a VLAN that was not created on the system.

Add a MAC-Based VLAN Group

➢ **To add a MAC-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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > VLAN > Advanced > MAC Based VLAN Group Configuration**.

   The MAC Based VLAN Group Configuration page displays. The page also shows the MAC Based VLAN Mapping section.

6. In the **MAC Address** field, enter a valid MAC address to be bound to a VLAN ID.

   This field is configurable only when a MAC-based VLAN is created.

7. In the **Prefix Mask** field, enter a value from 9 to 48.
8. In the **Group ID** field, specify a group ID that allows you to identify the group.
9. Click the **Add** button.

   The MAC address is added to the MAC-based VLAN group.

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

Table 24. MAC Based VLAN Mapping

Field	Definition
Group ID	The ID of the group.
VLAN ID	The VLAN ID that is associated with the group.
Ports	The ports that are assigned to the VLAN as a result of MAC-based VLAN mapping.

Delete a MAC-Based VLAN Group

➢ **To delete a MAC-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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > VLAN > Advanced > MAC Based VLAN Group Configuration**.

   The MAC Based VLAN Group Configuration page displays.
6. Select the check box for the group that you want to remove.
7. Click the **Delete** button.

   The MAC-based VLAN group is removed.

Manually Add Members to or Remove Them From a MAC-Based VLAN Group

➢ **To add members to or remove them from a MAC-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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > VLAN > Advanced > MAC Based VLAN Group Membership**.

   The MAC Based VLAN Group Membership page displays.

6. In the **Group ID** menu, select the group ID.
7. In the **VLAN ID** menu, select the VLAN ID.
8. In the Ports table, click the port once to add it to the VLAN for the group or twice to remove it from the VLAN for the group.

   By default, the selection is blank, which means that the port is excluded from the VLAN for the group.

9. In the LAG table, click the LAG once to add it to the VLAN for the group or twice to remove it from the VLAN for the group.

   By default, the selection is blank, which means that the LAG is excluded from the VLAN for the group.

10. Click the **Apply** button.

    Your settings are saved.

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 received on that port for that protocol are assigned the protocol-based VLAN ID. Untagged frames received 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 using the Port VLAN Configuration page.

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 group ID.

➢ **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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration**.

   The Protocol Based VLAN Group Configuration page displays. The page also shows the Protocol Based VLAN Mapping section.

6. In the **Group ID** field, specify a group ID that allows you to identify the group.
7. In the **Protocol** field, enter one or more protocols that must be associated with the group.

   You can enter the ARP, IP, and IPX keywords. Separate keywords with a comma. Although you cannot enter other keywords, you can enter hexadecimal or decimal values in the range of 0x0600 (1536) to 0xFFFF (65535).

8. Click the **Add** button.

   The protocol-based VLAN group is added to the switch.

9. Click the **Apply** button.

   Your settings are saved.

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

Table 25. Protocol Based VLAN Mapping

Field	Definition
Group ID	The ID of the group.
VLAN ID	The VLAN ID that is associated with the group.
Ports	The ports that are assigned to the VLAN as a result of protocol-based VLAN mapping.

Delete a Protocol-Based VLAN Group

➢ **To delete 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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration**.

   The Protocol Based VLAN Group Configuration page displays.
6. Select the check box for the group that you want to remove.
7. Click the **Delete** button.

   The protocol-based VLAN group is removed.

Manually Add Members to or Remove Them From a Protocol-Based VLAN Group

➢ **To add members to or remove them from 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Membership**.

   The Protocol Based VLAN Group Membership page displays.

6. In the **Group ID** menu, select the group ID.
7. In the **VLAN ID** menu, select the VLAN ID.
8. In the Ports table, click the port once to add it to the VLAN for the group or twice to remove it from the VLAN for the group.

   By default, the selection is blank, which means that the port is excluded from the VLAN for the group.

9. In the LAG table, click the LAG once to add it to the VLAN for the group or twice to remove it from the VLAN for the group.

   By default, the selection is blank, which means that the LAG is excluded from the VLAN for the group.

10. Click the **Apply** button.

    Your settings are saved.

Configure GARP Switch Settings

The Generic Attribute Registration Protocol (GARP) is used to exchange information between GARP participants to register and deregister attribute values within a bridged LAN. When a GARP participant declares or withdraws a given attribute, the attribute value is recorded with the applicant state machine for that attribute, for the port from which the declaration or withdrawal was made.

- Registration occurs only on ports that receive the GARP PDU containing a declaration or withdrawal.
- Deregistration occurs only if all GARP participants connected to the same LAN segment as the port withdraw the declaration.

GARP is part of the IEEE 802.1p extension to its 802.1D (spanning tree) specification. It includes the following:

- **GARP Information Declaration (GID)**. The part of GARP that generates data.
- **GARP Information Propagation (GIP)**. The part of GARP that distributes data.

Note: It can take up to 10 seconds for GARP configuration changes to take effect.

➢ **To configure GARP switch 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > VLAN > Advanced > GARP Switch Configuration**.

   The GARP Switch Configuration page displays.

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

   This selects the GARP VLAN registration protocol administrative mode for the switch. The default is Disable.

7. Click the **Apply** button.

   Your settings are saved.

Configure GARP Ports

Note: It can take up to 10 seconds for GARP configuration changes to take effect.

➢ **To configure GARP 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 *Access the Switch* on page 12.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > VLAN > Advanced > GARP Port Configuration**.

   The GARP Port Configuration page displays.

6. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
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 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.
8. From the **GVRP State** menu, select **Enable** or **Disable**.

   This specifies the GARP VLAN registration protocol administrative mode for the port. If you select **Disable**, the protocol is not active and the join time, leave time, and leave all time options are without any effect. The default is Disable.

9. In the **Join Timer** field, specify the time in centiseconds between the transmission of GARP PDUs registering (or reregistering) membership for a VLAN or multicast group.

   Enter a number between 10 and 100 (0.1 to 1.0 seconds). The default is 20 centiseconds (0.2 seconds). An instance of this timer exists for each GARP participant for each port.

10. In the **Leave Timer** field, specify the time in centiseconds to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry.

    This allows time for another station to assert registration for the same attribute to maintain uninterrupted service. Enter a number between 20 and 600 (0.2 to 6.0 seconds). The default is 60 centiseconds (0.6 seconds). An instance of this timer exists for each GARP participant for each port.

11. In the **Leave All Timer field**, specify how frequently (in centiseconds) LeaveAll PDUs are generated.

    A LeaveAll PDU indicates that all registrations will be deregistered soon. To maintain registration, participants must rejoin. The leave all period timer is set to a random value in the range of LeaveAllTime to 1.5 x LeaveAllTime. The timer is specified in centiseconds. Enter a number between 200 and 6000 (2 to 60 seconds). The default is 1000

centiseconds (10 seconds). An instance of this timer exists for each GARP participant for each port.

12. Click the **Apply** button.

    Your settings are saved.

Configure a Voice VLAN

You can configure the global settings for a voice VLAN and enable or disable the voice VLAN for specific ports and LAGs that carry traffic from IP phones.

The voice VLAN feature can help ensure that the sound quality of an IP phone is safeguarded from deteriorating when the data traffic on the port is high.

The following are two operational modes for IP phones:

- IP phones are configured with VLAN mode enabled, ensuring that the phone uses tagged packets for all communications.
- IP phones are configured with VLAN mode disabled, ensuring that the phone uses untagged packets for all communications. The phone uses untagged packets while retrieving the initial IP address through DHCP. The phone eventually uses the voice VLAN and commences sending tagged packets.

From the **Switching > Voice VLAN > Advanced** menu, you can access pages that are described in the following sections:

- *Configure the Global Voice VLAN Settings* on page 110
- *Configure Membership for the Voice VLAN* on page 111
- *Configure the Global Voice VLAN Settings* on page 110

Configure the Global Voice VLAN Settings

➢ **To configure the global voice VLAN 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Voice VLAN > Properties**.

   The Properties page displays.

6. Select the Voice VLAN Status **Enable** radio button.

   This enables the administrative mode for the voice VLAN for the switch. The default is Disable.

7. In the **Voice VLAN ID** menu, select the VLAN that must be the voice VLAN.

   VLAN 1, the default VLAN, cannot be the voice VLAN.

8. In the **Class Of Service** menu, select the CoS tag value from 0 to 7 that must be reassigned for packets that are received on the voice VLAN when Remark CoS is enabled.

   The default value is 6.

9. To enable Class of Service remarking on the ports and LAGs that are members of the voice VLAN, select the Remark CoS **Enable** radio button.

   By default, Remark CoS is disabled.

10. In the **Voice VLAN Aging Time** fields, specify the time after which the last IP phone's OUI must expire for the ports and LAGs that are members of the voice VLAN.

    By default, the OUI expires after 1 day.

11. Click the **Apply** button.

    Your settings are saved.

Configure Membership for the Voice VLAN

➢ **To add or remove interfaces from the 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Voice VLAN > Advanced > Port Setting**.

   The Port Settings page displays.

6. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
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 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.
8. From the **Voice VLAN Mode** menu, select one of the following options:
   - **Enable**. Adds the selected interfaces to the voice VLAN.
   - **Disable**. Removes the selected interfaces from the voice VLAN. The default is Disable.
9. Click the **Apply** button.

   Your settings are saved.

   The Membership field displays whether the current operational status of the voice VLAN on the interface is active or not.

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
- 00:04:0D: AVAYA1
- 00:12:43: CISCO2
- 00:1B:4F: AVAYA2
- 00:60:B9: NITSUKO
- 00:D0:1E: PINTEL
- 00:E0:75: VERILINK
- 00:E0:BB: 3COM

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

Add VoIP OUI Prefixes

➢ **To add VoIP OUI prefixes to 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Voice VLAN > Advanced > OUI**.

   The OUI page displays.

6. In the **Telephony OUI(s)** field, specify the VoIP OUI prefix to be added in the format AA:BB:CC.
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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Voice VLAN > Advanced > OUI**.

The OUI page displays.

6. Select the check box for each OUI prefix to be removed.
7. Click the **Delete** button.

   The telephony OUI entries are removed.

Configure Auto-VoIP

Voice over Internet Protocol (VoIP) enables telephone calls over a data network. Because voice traffic is typically more time-sensitive than data traffic, the Auto-VoIP feature helps to provide a classification mechanism for voice packets so that they can be prioritized above data packets in order to provide better Quality of Service (QoS). With the Auto-VoIP feature, voice prioritization is provided based on call-control protocols (SIP, SCCP, H.323) or OUI bits.

To prioritize time-sensitive voice traffic over data traffic, protocol-based Auto-VoIP checks for packets carrying the following VoIP protocols:

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

All three protocols are checked during the signaling and call identification stage. Once the VoIP call is established, only the SIP and SCCP protocols are checked. This feature supports up to 48 bidirectional VoIP calls.

VoIP frames that are received on ports for which the Auto-VoIP feature is enabled are assigned to queue 6.

The Auto-VoIP, QoS CoS, and QoS DiffServ features can coexist and be activated at the same time. If these features are active at the same time on the same port, the manual QoS assignment might override the VoIP QoS assignment.

➢ **To configure Auto-VoIP on 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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Auto-VoIP**.
6. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
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 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.
8. From the **Auto-VoIP Mode** menu, select one of the following options:
   - **Enable**. Enables Auto-VoIP on the selected interfaces.
   - **Disable**. Disables Auto-VoIP on the selected interfaces. The default is Disable.
9. Click the **Apply** button.

   Your settings are saved.

   The Traffic Class fields show 6, which is the default queue to which the interfaces are assigned.

Configure Spanning Tree Protocol

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

Classic STP provides a single path between end stations, avoiding and eliminating loops. For information on configuring Common STP, see *Configure CST Port Settings* on page 120.

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

Note: For two bridges to be in the same region, the force version must be 802.1s and their configuration names, digest keys, and revision levels must match. For additional information about regions and their effect on network topology, refer to the IEEE 802.1Q standard.

From the **Switching > STP > Advanced** menu, you can access pages that are described in the following sections:

- *Configure STP Settings* on page 116
- *Configure CST Settings* on page 118
- *Configure CST Port Settings* on page 120
- *View the CST Port Status* on page 121
- *View Rapid STP Information* on page 123
- *Manage MST Settings* on page 124
- *Configure MST Port Settings* on page 126
- *View STP Statistics* on page 129

Configure STP Settings

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

➢ **To configure STP settings:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

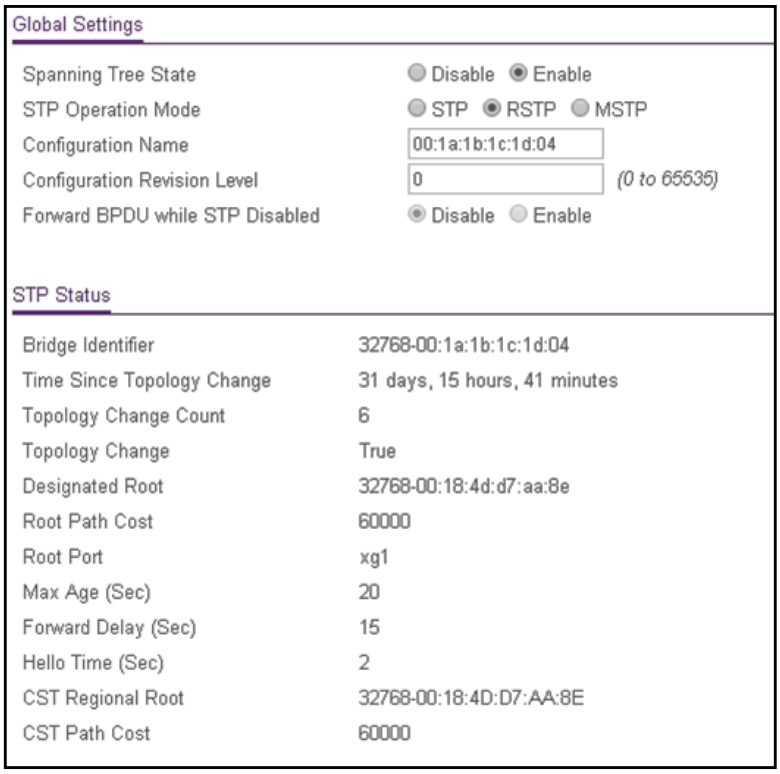
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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



6. Configure the following settings:
   - **Spanning Tree State**. Enable or disable the spanning tree operation on the switch.
   - **STP Operation Mode**. Specify the STP version for the switch. The options are **STP**, **RSTP**, and **MSTP**.
   - **Configuration Name**. Specify an identifier used to identify the configuration currently being used. It can be up to 32 alphanumeric characters.
   - **Configuration Revision Level**. Specify an identifier used to identify the configuration currently being used. The values allowed are between 0 and 65535. The default value is 0.
   - **Forward BPDU while STP Disabled**. Enable or disable the BPDU Flood. This setting specifies whether spanning tree BPDUs are forwarded or not while spanning tree is disabled on the switch.
7. Click the **Apply** button.

   Your settings are saved.

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

Table 26. STP Status

Field	Description
Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	The time in day-hour-minute-second format since the topology of the CST last changed.
Topology Change Count	The number of times that the topology changed for the CST.
Topology Change	The value of the topology change parameter for the switch indicating whether a topology change is in progress on any port assigned to the CST. Possible values are True and False.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Path cost to the designated root for the CST.
Root Port	Port to access the designated root for the CST.
Max Age (Secs)	The maximum age timer controls the maximum length of time in seconds that passes before a bridge port saves its configuration BPDU information.
Forward Delay (Secs)	The derived value of the Root Port Bridge Forward Delay parameter.
Hello Time (Secs)	Minimum time in seconds between the transmission of configuration BPDUs.
CST Regional Root	Priority and base MAC address of the CST regional root.
CST Path Cost	Path cost to the CST tree regional root.

Configure CST Settings

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

➢ **To configure CST settings:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

The default password is **password**.

The System Information page displays.

5. Select **Switching > STP > Advanced > CST Configuration**.

   The CST Configuration page displays. The page also shows the MSTP Status section.

6. Specify the CST options:
   - **Bridge Priority**. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. Specify the bridge priority value for the Common and Internal Spanning Tree (CST). The valid range is 0–61440. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if you set the priority to any value between 0 and 4095, the switch automatically sets the value to 0. The default 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 valid range is 6–40, and the value must be less than or equal to (2 * Bridge Forward Delay) – 1 and greater than or equal to 2 * (Bridge Hello Time +1). The default value is 20.
   - **Bridge Hello Time (secs)**. 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 valid range is 6–40. The default is 20 hops.

7. Click the **Apply** button.

   Your settings are saved.

The following table describes the MSTP Status information that is displayed.

Table 27. STP advanced CST configuration, MSTP status

Field	Description
MST ID	The ID of the MST instance (including the CST).
VID	The VLAN IDs that are associated with the MST ID.
FID	The filtering identifiers (FIDs) that are associated with the MST ID.

Configure CST Port Settings

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

➢ **To configure CST port settings:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > STP > Advanced > CST Port Configuration**.

   The Port Configuration page displays.

6. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
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 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.
8. From the **STP Status** menu, select the option to enable or disable spanning tree administrative mode associated with the port or port channel.

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

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

   The possible values are **Enable**, **Disable**, and **Auto**. The default value is Auto, which specifies that the switch waits three seconds (with no BPDUs received on the interface) before placing the interface into the PortFast mode.

10. From the **BPDU Forwarding** menu, configure BPDU forwarding.

The possible values are **Enable** and **Disable**. The default value is Disable. When BPDU forwarding is enabled, the switch forwards the BPDU traffic arriving on this port when STP is disabled on this port.

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 of 0 to 200000000. The default is 0. When the path cost is set to 0, the value is updated with the external path cost from a received STP packet.

12. In the **Priority** field, specify the priority for a particular port within the CST.

    The port priority is set in multiples of 16. The range is 0 to 240. The possible values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, or 240. The default value is 128.

13. Click the **Apply** button.

    Your settings are saved.

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

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

Table 28. CST port configuration

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

View the CST Port Status

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

➢ **To 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

The System Information page displays.

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

   The CST Port Status page displays.

6. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
7. To refresh the page with the latest information about the switch, click the **Refresh** button.

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

Table 29. CST port status

Field	Description
Interface	Identify the physical or port channel interfaces associated with VLANs associated with the CST.
Port Role	Each MST bridge port that is enabled is assigned a port role for each spanning tree. The port role is one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.
Designated Root	Root bridge for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	Path cost offered to the LAN by the designated port.
Designated Bridge	Bridge identifier of the bridge with the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	Port identifier on the designated bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.
Edge port	Indicates whether the port is enabled as an edge port. It is either Enabled or Disabled.
Point-to-point MAC	Derived value of the point-to-point status.
CST Regional Root	Bridge identifier of the CST regional root. It is made up using the bridge priority and the base MAC address of the bridge.
CST Path Cost	Path cost to the CST regional root.
Port Forwarding State	The forwarding state of the port.

View Rapid STP Information

Use the Rapid STP page to view information about 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > STP > Advanced > RSTP**.

   The Rapid STF page displays.

6. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
7. To refresh the page with the latest information about the switch, click the **Refresh** button.

The following table describes the Rapid STP Status information displayed on the page.

Table 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 is one of the following: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.
Mode	Specifies the spanning tree operation mode. Different modes are STP, RSTP, and MSTP.
Fast Link	Indicates whether the port is enabled as an edge port.
Status	The forwarding state of this port.

Manage MST Settings

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

Configure an MST Instance

➢ **To configure an MST instance:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > STP > Advanced > MST Configuration**.

6. Configure the MST values:
   - **MST ID**. Specify the ID of the MST to create. The valid values for this are 1 to 15.
   - **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. The valid range is 0–61440. The default value is 32768.
   - **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.
Time Since Topology Change	The time 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 parameter for the switch indicating if a topology change is in progress on any port assigned to the selected MST instance. It is either True or False.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge
Root Path Cost	Path cost to the designated root for this MST instance.
Root Port	Port to access the designated root for this MST instance.

Modify an MST Instance

➢ **To modify an MST instance:**

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > STP > Advanced > MST Configuration**.

   The MST Configuration page displays.
6. Select the check box for the instance.

   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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > STP > Advanced > MST Configuration**.

   The MST Configuration page displays.
6. Select the check box for the instance.
7. Click the **Delete** button.

   The MST instance is removed.

Configure MST Port Settings

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

➢ **To configure MST port settings and start the STP migration process 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.

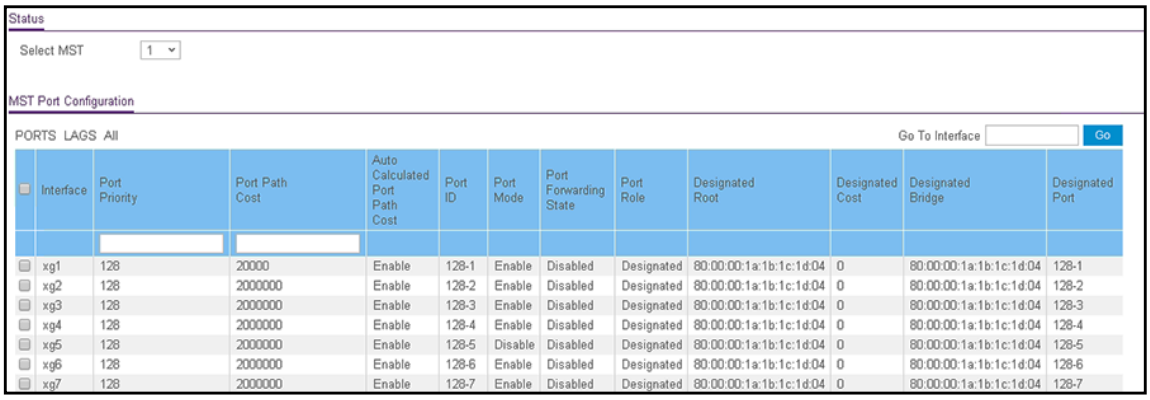
   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

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

   The default password is **password**.

The System Information page displays.

5. Select **Switching > STP > Advanced > MST Port Configuration**.



6. In the **MST Select** menu, select the MST instance.
7. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the interface, or type the interface number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. Configure the MST values for the selected interfaces:
   - **Port Priority**. Specify the priority for the interfaces. The port priority is set in multiples of 16. The range is 0–240. The default setting is 128.
   - **Port Path Cost**. Specify the path cost for the interfaces. The range is 0–200000000. The default setting is 2000000. If you enter 0, the switch recalculates the path cost.
10. Click the **Apply** button.

    Your settings are saved.
11. To restart the STP migration process (that is, force renegotiation with neighboring switches for the selected interfaces), click the **Activate Protocol Migration** 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	Displays whether the path cost is automatically calculated (Enabled) or not (Disabled). Path cost is calculated based on the link speed of the port if the configured value for Port Path Cost is 0.
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 Mode	Spanning Tree Protocol administrative mode associated with the port or port channel. Possible values are Enable or Disable.
Port Forwarding State	Indicates the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are as follows: • **Disabled**. STP is currently disabled on the port. The port forwards traffic while learning MAC addresses. • **Blocking**. The port is currently blocked and cannot be used to forward traffic or learn MAC addresses. • **Listening**. The port is currently in the listening mode. The port cannot forward traffic nor can it learn MAC addresses. • **Learning**. The port is currently in the learning mode. The port cannot forward traffic. However, it can learn new MAC addresses. • **Forwarding**. The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses
Port Role	Each MST bridge port that is enabled is assigned a port role for each spanning tree. The port role is one of the following: Root, Designated, Alternate, Backup, Master, or Disabled Port.
Designated Root	Root bridge for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	Displays cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
Designated Bridge	Bridge identifier of the bridge with the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	Port identifier on the designated bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.

View STP Statistics

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

➢ **To view Spanning Tree statistics:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > STP > Advanced > STP Statistics**.

   The STP Statistics page displays.

6. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
7. To refresh the page with the latest information about the switch, click the **Refresh** button.

The following table describes the information available about the STP Statistics page.

Table 33. STP Statistics

Field	Description
Interface	The physical port or LAG.
STP BPDUs Received	The number of STP BPDUs received at the port or LAG.
STP BPDUs Transmitted	The number of STP BPDUs transmitted from the port or LAG.

Configure Multicast

Multicast IP traffic is traffic that is destined to a host group. Host groups for IPv4 multicast are identified by class D addresses, which range from 224.0.0.0 to 239.255.255.255. Host groups for IPv6 multicast are identified by the prefix ff00::/8.

When you limit multicast transmissions to only certain ports on the switch, traffic is not forwarded to parts of the network where it is not needed.

From the **Switching > Multicast** menu, you can access pages that are described in the following sections:

- *View the MFDB Table* on page 130
- *View the MFDB Statistics* on page 132
- *Configure Auto-Video* on page 132
- *IGMP Snooping Overview* on page 133
- *Configure the Global IGMP Snooping Settings* on page 134
- *View the IGMP Snooping Table* on page 135
- *Configure IGMP Snooping for VLANs* on page 136
- *Modify IGMP Snooping Settings for a VLAN* on page 137
- *Disable IGMP Snooping on a VLAN and Remove It From the Table* on page 138
- *IGMP Snooping Querier Overview* on page 138
- *Configure IGMP Snooping Querier* on page 139
- *Configure IGMP Snooping Querier for VLANs* on page 140
- *Display the IGMP Snooping Querier for VLAN Status* on page 141
- *MLD Snooping Overview* on page 142
- *Configure the Global MLD Snooping Settings* on page 142
- *Configure MLD Snooping for a VLAN* on page 143
- *Configure a Multicast Router Interface on a VLAN* on page 144
- *Configure MLD Snooping Querier* on page 145
- *Configure MLD Snooping Querier VLAN Settings* on page 146
- *Configure a Multicast Group* on page 147
- *Configure Multicast Group Membership* on page 149
- *Configure the Multicast Forward All Option* on page 150

View the MFDB Table

The Layer 2 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.

When the switch receives a packet with a destination multicast MAC address, this address is combined with the VLAN ID, and the switch performs a search in the MFDB. If no match is found, the packet is either flooded to all ports in the VLAN or discarded, depending on the switch configuration. If a match is found, the packet is forwarded only to the ports that are members of that multicast group per the specific VLAN ID.

To view the MFDB Table:

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Multicast > MFDB > MFDB Table**.

   The MFDB Table page displays.
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.

The following table displays the MFDB table information.

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.
Component	The component through which the entry was added to the Multicast Forwarding Database. Possible values are IGMP Snooping, Static Filtering, and MLD Snooping.
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. Possible values are Management Configured, Network Configured, and Network Assisted.
Interface	The interfaces that are designated for forwarding (Fwd:) and filtering (Flt:) for the selected address.
Forwarding Interfaces	The resultant forwarding list is derived from combining all the forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

View the MFDB Statistics

➢ **To view the MFDB statistics:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > MFDB > MFDB Statistics**.

   The MFDB Statistics page displays.

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.
Current Entries	The current number of entries in the Multicast Forwarding Database table.

Configure Auto-Video

If the switch supports devices or applications running multicast traffic, the Auto-Video feature simplifies IGMP snooping querier configuration, such as video surveillance cameras.

➢ **To configure auto-video 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > Auto-Video**.

   The Auto-Video Configuration page displays.

6. Select one of the following radio buttons:
   - Select the **Disable** radio button to globally disable Auto-Video administrative mode for the switch.
   - Select the **Enable** radio button to globally enable Auto-Video administrative mode for the switch.
7. If you enable the feature, from the **Auto-Video VLAN** menu, select the ID of the VLAN that must become the Auto-Video VLAN.
8. Click the **Apply** button.

   Your settings are saved.

IGMP Snooping Overview

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

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

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

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

Configure the Global IGMP Snooping Settings

Before IGMP snooping can be enabled on specific VLANs (see *Configure IGMP Snooping for VLANs* on page 136), you must configure the global settings.

➢ **To configure the global IGMP 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping Configuration**.

   The IGMP Snooping Configuration page displays. The page also shows the VLAN IDs Enabled For IGMP Snooping section and the VLAN IDs Enabled For IGMP Snooping Querier section.

6. Next to IGMP Snooping Status, select whether IGMP snooping is enabled on the switch:
   - **Enable**. The switch snoops all IGMP packets it receives to determine which segments should receive packets directed to the group address.
   - **Disable**. The switch does not snoop IGMP packets. This is the default setting.
7. Next to Block Unknown Multicast Addresses, select whether unknown multicast addresses are blocked:
   - **Enable**. Packets with unknown multicast MAC addresses in the destination field are dropped.
   - **Disable**. Packets with unknown destination multicast MAC addresses are flooded to all interfaces in VLAN. This is the default setting.
8. Click the **Apply** button.

   Your settings are saved.

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

The following table displays information about the global IGMP snooping status.

Table 36. IGMP snooping and IGMP snooping querier VLAN information

Field	Description
VLAN IDs Enabled For IGMP Snooping	The VLANs on which IGMP snooping is enabled. For more information, see *Configure IGMP Snooping for VLANs* on page 136.
VLAN IDs Enabled For IGMP Snooping Querier	The VLANs on which IGMP snooping querier is enabled. For more information, see *Configure MLD Snooping Querier VLAN Settings* on page 146.

View the IGMP Snooping Table

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

➢ **To view the entries in the IGMP snooping table:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping Table**.

   The IGMP Snooping Table page displays.

6. In the **Search By MAC Address** field, specify the MAC address whose MFDB table entry you want to view.

   Enter six two-digit hexadecimal numbers separated by colons, for example, 00:01:23:43:45:67.

7. Click the **Go** button.

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

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 information, filtering information, or both. The format is six 2-digit hexadecimal numbers that are separated by colons, for example, 01:00:5e:45:67:89.
VLAN ID	The VLAN for which the switch holds forwarding and filtering information.
Type	The type of the entry. Static entries were manually configured. Dynamic entries were added to the table as a result of a learning process or protocol.
Description	The text description for the multicast table entry. Possible values 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

You can configure the parameters for IGMP snooping, which is used to build forwarding lists for multicast traffic.

➢ **To configure IGMP snooping 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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping VLAN Configuration**.

   The IGMP Snooping VLAN Configuration page displays.
6. From the **VLAN ID** menu, select the VLAN.
7. From the **Fast Leave Admin Mode** menu, select whether IGMP snooping Fast Leave mode is enabled.

Enabling Fast Leave mode lets the switch immediately remove the Layer 2 LAN interfaces from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending MAC-based general queries to the interface.

We recommend that you enable fast leave admin mode only on VLANs for which only one host is connected to a Layer 2 LAN port. This mode prevents the inadvertent dropping of the other hosts that are connected to the same Layer 2 LAN port but are configured to receive multicast traffic. Also, fast leave processing is supported only with IGMP version 2 hosts.

8. In the **Max Response Time** field, enter the period in seconds that the switch must wait after it sends a query on the VLAN because it did not receive a report for a particular group. The valid range is 5–20 seconds. The default value is 10.
9. From the **Query Mode** menu, select whether the IGMP querier mode is enabled.
10. In the **Query Interval** field, enter the value for the interval between IGMP queries. The valid range is 30–1800 seconds. The default is 125 seconds.
11. Click the **Apply** button.

    Your settings are saved.

The following table displays nonconfigurable information about IGMP snooping for VLANs.

Table 38. IGMP VLAN snooping information

Field	Description
Host Timeout	The period that the switch must wait for a report for a particular group on a particular interface before it deletes that interface from the group. This value is calculated as follows: (Query Interval * 2) + Maximum Response Time.
MRouter Timeout	The period 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. This value is calculated as follows: Query Interval * 2.

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 *Access the Switch* on page 12.

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

   The default password is **password**.

The System Information page displays.

5. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping VLAN Configuration**.

   The IGMP Snooping VLAN Configuration page displays.

6. Select the check box for the VLAN ID.
7. Update the values.
8. Click the **Apply** button.

   Your settings are saved.

Disable IGMP Snooping on a VLAN and Remove It From the Table

➢ **To disable IGMP snooping on a VLAN and remove it from the 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping VLAN Configuration**.

   The IGMP Snooping VLAN Configuration page displays.

6. Select the check box for the VLAN ID.
7. Click the **Delete** button.

   Snooping is disabled on the VLAN and the VLAN is removed from the table.

IGMP Snooping Querier Overview

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

You can configure and display information about IGMP snooping queriers on the network and, separately, on VLANs.

Configure IGMP Snooping Querier

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

➢ **To configure IGMP snooping querier settings:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > IGMP Snooping Querier > Querier Configuration**.

   The Querier Configuration page displays. The page also shows the VLAN IDs Enabled for IGMP Snooping Querier section.

6. Next to Querier Admin Mode, select whether the IGMP snooping querier is enabled on the switch:
   - **Enable**. The switch queries devices on the network for IGMP reports.
   - **Disable**. The switch does not query devices on the network for IGMP reports. This is the default setting.
7. Configure the following settings:
   - **Snooping Querier 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.
   - **Query Interval (secs)**. Specify the interval in seconds between periodic queries sent by the snooping querier. The query interval must be a value in the range of 30–1800. The default value is 125.
8. Click the **Apply** button.

   Your settings are saved.

The following table displays nonconfigurable information about the IGMP snooping querier.

Table 39. IGMP snooping querier information

Field	Description
IGMP Version	The IGMP protocol version used in periodic IGMP queries. Only ICMPv2 is supported.
Querier Expiry Interval	The interval in seconds after which the last querier information is removed. This value is calculated as follows: 2 * Query Interval + 5, so by default the value is 2*125+5 = 255.
VLAN IDs Enabled For IGMP Snooping Querier	The VLANs on which the IGMP snooping querier is enabled. For more information, see *Configure MLD Snooping Querier VLAN Settings* on page 146.

Configure IGMP Snooping Querier for VLANs

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

➢ **To create a new VLAN ID for IGMP snooping:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Configuration**.

   The Querier VLAN Configuration page displays.

6. From the **VLAN ID** menu, select **New Entry**.
7. Configure the following settings:
   - **VLAN ID**. The VLAN ID for which the IGMP snooping querier is to be enabled.
   - **Querier Election Participate Mode**. Enable or disable querier this mode:
     - **Disable**. Upon seeing another querier of the same version in the VLAN, the snooping querier moves to the non-querier state.
     - **Enable**. The snooping querier participates in querier election, in which the lowest IP address operates as the querier in that VLAN. The other querier moves to non-querier state.

- **Snooping Querier VLAN Address**. Specify the snooping querier IP address to be used as the source address in periodic IGMP queries sent on the specified VLAN.

8. Click the **Apply** button.

   Your settings are saved.

Display the 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > IGMP Snooping Querier > Querier VLAN Status**.

   The Querier VLAN Status page displays.

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

Table 40. 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: • **Enabled**. The snooping switch is the querier in the VLAN. The snooping switch sends periodic queries with a time interval equal to the configured querier query interval. • **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 snooping querier.
Operational Max Response Time	The maximum response time used in the queries that are sent by the snooping querier.

MLD Snooping Overview

Multicast Listener Discovery (MLD) is a protocol that is used by IPv6 multicast routers to discover the presence of multicast listeners (nodes that want to receive IPv6 multicast packets) on its directly attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD version 1 (MLDv1) is equivalent to IGMPv2, and MLD version 2 (MLDv2) is equivalent to IGMPv3.

MLD is a subprotocol of Internet Control Message Protocol version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages, identified in IPv6 packets by a preceding Next Header value of 58.

The switch can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data based on destination IPv6 multicast MAC addresses. You can configure the switch to perform MLD snooping and IGMP snooping simultaneously.

In IPv4, Layer 2 switches can use IGMP snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast address. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. The switch constructs this list by snooping IPv6 multicast control packets.

The switch uses MLD snooping to build a forwarding list for multicast traffic.

Configure the Global MLD Snooping Settings

You can enable MLD snooping globally.

➢ **To enable MLD snooping 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > MLD Snooping > Configuration**.

   The MLD Snooping Configuration page displays. The page also displays the VLAN IDs Enabled for MLD Snooping section.

6. Select the MLD Snooping Admin Mode **Enable** radio button.

   By default, the Disable radio button is selected.

7. Click the **Apply** button.

   Your settings are saved.

   The VLAN IDs Enabled For MLD Snooping section displays the VLAN IDs, if any, for which MLD snooping is enabled.

Configure MLD Snooping for a VLAN

When you enable MLD snooping globally (see *Configure the Global MLD Snooping Settings* on page 142), you can enable MLD snooping on a per-VLAN basis.

➢ **To configure MLD snooping 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > MLD Snooping > MLD VLAN Configuration**.

   The MLD VLAN Configuration page displays.

6. From the **VLAN ID** menu, select the VLAN ID.
7. From the **Admin Mode** menu, select **Enable**.
8. From the **Fast Leave Admin Mode** menu, select to enable or disable the MLD snooping Fast Leave mode.

   Enabling Fast Leave mode lets the switch immediately remove the Layer 2 LAN interfaces from its forwarding table entry upon receiving an MLD Done message for that multicast group without first sending MAC-based general queries to the interface.

   We recommend that you enable Fast Leave admin mode only on VLANs for which only one host is connected to a Layer 2 LAN port. This mode prevents the inadvertent dropping of the other hosts that are connected to the same Layer 2 LAN port but are configured to receive multicast traffic. Also, fast leave processing is supported only with MLD version 1 hosts.

9. In the **Group Membership Interval** field, set the value for the group membership interval of MLD snooping.

   The valid range is 4 to 3620 seconds. The default value is 260 seconds.

10. In the **Maximum Response Time** field, set the value for the maximum response time of MLD snooping.

    The valid range is 1 to 20 seconds. The default value is 20 seconds. This value must be shorter than the group membership interval value.

11. Click the **Add** button.

    MLD snooping is enabled on the specified VLAN.

    The Multicast Router Expiry Time field is a calculated field, displaying the value for the multicast router expiration time of MLD snooping for the specified VLAN ID. This value is calculated as the value in the Group Membership Interval field minus the value in the Maximum Response Time field.

Configure a Multicast Router Interface on a VLAN

When you connect an external multicast router to a switch interface that is a member of a VLAN and you configure that switch interface as a multicast router interface, the external multicast router is automatically added to the list of learned multicast routers.

This dynamic learning mode is applicable only to multicast router information (that is, to queries from an attached true querier). In such a situation, you do not need to enable a snooping dynamic learning mode (that is, the snooping interface mode or the snooping VLAN mode) for the multicast router interface.

➢ **To configure a multicast router interface 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > MLD Snooping > Multicast Router VLAN Configuration**.

   The Multicast Router VLAN Configuration page displays.

6. From the **Interface** menu, select the multicast router interface.

This is the interface to which an external multicast router is connected.

7. From the **VLAN ID** menu, select the VLAN ID of which the interface must be a member.
8. From the **Multicast Router** menu, select **Enable** to enable the multicast router mode for the VLAN (and therefore, for the multicast router interface).

   By default, Disable is selected.
9. Click the **Apply** button.

   Your settings are saved.

Configure MLD Snooping Querier

You can configure the settings for an MLD snooping querier.

➢ **To configure an MLD 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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Multicast > MLD Snooping > Querier Configuration**.

   The MLD Snooping Querier Configuration page displays. The page also shows the VLAN IDs Enabled for MLD Snooping Querier section.
6. Configure the following settings:
   - **Querier Admin Mode**. Enable or disable MLD snooping for the switch. The default is Disable.
   - **Snooping Querier Address**. Enter an IPv6 address that is used as the source address in periodic MLD queries. This address is used when no address is configured on the VLAN on which a query is sent. The supported IPv6 address formats are x:x:x:x:x:x:x:x and x::x.
   - **MLD Version**. This is a field with the fixed value 1, which indicates that MLDv1 is the version that is used in periodic MLD queries.
   - **Query Interval (secs)**. Specify the time interval in seconds between periodic queries sent by the snooping querier. The query interval must be a value in the range of 30 to 1800. The default value is 125.

- **Querier Expiry Interval (secs)**. This is a field with a calculated value that shows the interval in seconds after which the last querier information is removed. The interval is calculated as 2 * Query Interval + 5. The default value is 255.

7. Click the **Apply** button.

   Your settings are saved.

   The VLAN IDs Enabled for MLD Snooping Querier section displays the IDs of the VLANs for which MLD snooping querier is enabled (see *Configure MLD Snooping Querier VLAN Settings* on page 146).

Configure MLD Snooping Querier VLAN Settings

➢ **To configure MLD snooping querier VLAN 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > MLD Snooping > Querier VLAN Configuration**.

   The MLD Snooping Querier VLAN Configuration page displays.

6. In the **VLAN ID** field, specify the VLAN ID on which the MLD snooping querier is administratively enabled.
7. From the **Querier Election Participate Mode** menu, select to enable or disable the querier participation election mode for MLD snooping.

   When this mode is disabled, on detecting another querier of same version in the VLAN, the snooping querier moves to a non-querier state. When this mode is enabled, the snooping querier participates in querier election where the lowest IP address wins the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.

8. In the **Querier VLAN Address** field, specify the snooping querier address to be used as the source address in periodic MLD queries sent on the specified VLAN.
9. Click the **Apply** button.

   Your settings are saved.

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

Table 41. MLD Snooping Querier VLAN Configuration information

Field	Description
Operational State	The operational state of the MLD snooping querier on a VLAN. It can be in any of the following states: • **Enabled**. 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 detects a better (numerically lower) querier in the VLAN, it moves to non-querier mode. • **Disabled**. Snooping querier is not operational on the VLAN. The snooping querier moves to disabled mode when MLD 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 MLD 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 MLD 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.

Configure a Multicast Group

You can configure up to 512 static multicast groups. You create a multicast group by adding a multicast MAC address to a VLAN. The multicast MAC address becomes the group identifier.

➢ **To configure a multicast group:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > Static Multicast Address > Multicast Group Configuration**.

   The Multicast Group Configuration page displays.

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

   The multicast group is added.

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

Table 42. Multicast Group Configuration information

Field	Definition
VLAN Name	The VLAN name, if any, that is associated with the VLAN ID.
Type	The type of multicast group, which is determined by the way in which members are added to the group: • **Dynamic**. Members are added dynamically to the multicast group. By default, all groups are dynamic groups. • **Static**. If you add static members to the multicast group (see *Configure Multicast Group Membership* on page 149), the group becomes a static group.

Remove a Multicast Group

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

➢ **To remove one or more multicast groups:**

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Switching > Multicast > Static Multicast Address > Multicast Group Configuration**.

   The Multicast Group Configuration page displays.
6. Select the check boxes for the statically added multicast addresses that you want to remove.

You cannot select a check box for a dynamically added multicast address.

7. Click the **Delete** button.

   The multicast groups are removed.

Configure Multicast Group Membership

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

➢ **To configure multicast group membership:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > Static Multicast Address > Multicast Group Membership**.

   The Multicast Group Membership page displays. The page also displays the Multicast Group section.

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

   The Multicast Address of the VLAN is displayed and If a name is associated with the VLAN, the name displays in the VLAN Name field.

7. From the **Multicast Address** menu, select the MAC address that identifies the multicast group.
8. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
9. Select one or more interfaces by taking one of the following actions:

- To configure a single interface, select the check box associated with the interface, or type the interface number in the **Go To Interface** field and click the **Go** button.
- To configure multiple interfaces with the same settings, select the check box associated with each interface.
- To configure all interfaces with the same settings, select the check box in the heading row.

10. From the **Interface Status** menu, select one of the following options:
    - **Static**. The interface becomes a static member of the multicast group on the selected VLAN.
    - **Forbidden**. The interface is forbidden from joining the multicast group on the selected VLAN.
    - **Excluded**. The interface is not a static member of the multicast group but could become a dynamic member of a multicast group on the selected VLAN. This is the default state.

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

11. Click the **Apply** button.

    Your settings are saved.

Configure the Multicast Forward All Option

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

➢ **To enable the Multicast Forward All option for an interface:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Multicast > Static Multicast Address > Multicast Forward All**.

The Multicast Forward All page displays.

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

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

7. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
8. Select one or more interfaces by taking one of the following actions:
   - To configure a single interface, select the check box associated with the interface, or type the interface number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple interfaces with the same settings, select the check box associated with each interface.
   - To configure all interfaces with the same settings, select the check box in the heading row.
9. From the **Interface Status** menu, select one of the following options:
   - **Static**. The interface receives all multicast traffic on the VLAN and forwards the traffic.
   - **Forbidden**. The interface cannot receive any multicast traffic on the VLAN, even if the IGMP or MLD snooping process designated the interface as a member of a multicast group.
   - **Excluded**. The Multicast Forward All option is not enabled on the interface, that is, the interface does not forward all multicast traffic on the VLAN. This is the default state.
10. Click the **Apply** button.

    Your settings are saved.

View, Search, and Manage the MAC Address Table

The Address Table (or MAC Address Table) contains information about unicast MAC address entries for which the switch saved forwarding or filtering information. The transparent bridging function uses this information in determining how to propagate a received frame. Use the search function of the Address Table page to display information about the entries in the table.

You can also add static entries to the Address Table and specify the period after which dynamic MAC address entries that are not updated are automatically removed from the Address Table.

From the **Switching > Address Table > Advanced** menu, you can access pages that are described in the following sections:

- *View and Search the MAC Address Table* on page 152
- *Change the Aging-Out Period of Dynamic MAC Addresses* on page 153
- *Add a Static MAC Address* on page 154
- *Remove a Static MAC Address* on page 154

View and Search the MAC Address Table

➢ **To view and search 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Address Table > Address Table**.

   The Address Table page displays. The page also displays the MAC Address Table section.

6. From the **Search By** menu, select one of the following options:
   - **VLAN ID**. In the **Search By** field, enter a VLAN ID.
   - **Mac Address**. In the **Search By** field, enter a MAC address as six 2-digit hexadecimal numbers separated by colons, for example, 00:01:23:43:45:67.
   - **Interface**. In the **Search By** field, enter an interface number.
7. Click the **Go** button.

   If the searched value exists, the entry is displayed.

   Total MAC Addresses field shows the total number of MAC addresses in the MAC Address Table.

The following table describes the information in the MAC Address Table.

Table 43. MAC Address Table information

Field	Description
VLAN ID	The VLAN that is associated with the MAC address.
MAC Address	The MAC address. The format is six 2-digit hexadecimal numbers that are separated by colons, for example, 01:00:5e:45:67:89.
Interface	The interface that is associated with the MAC address.
Status	The type of the entry. Static entries were manually configured (see *Add a Static MAC Address* on page 154). Dynamic entries were added to the table as a result of a learning process or protocol.

Change the Aging-Out Period of Dynamic MAC Addresses

You can change the aging-out period after which a learned MAC address entry that is not updated is automatically removed from the forwarding database. By default, this period is 300 seconds. The forwarding database contains static entries, which never age out, and dynamically learned entries, which are removed if they are not updated before the aging-out period expires.

➢ **To change the aging-out period of dynamic 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Address Table > Address Table > Advanced > Dynamic Address**.

   The Dynamic Address page displays.

6. In the **Address Aging Timeout (seconds)** field, enter the aging-out period in seconds.

   The range is 10 to 500 seconds. The default is 300 seconds.

7. Click the **Apply** button.

   Your settings are saved.

Add a Static MAC Address

➢ **To add a static MAC address:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Switching > Address Table > Address Table > Advanced > Static MAC Address**.

   The Static MAC Address page displays.

6. From the **VLAN ID** menu, select a VLAN ID.
7. In the **MAC Address** field, enter the MAC address as six 2-digit hexadecimal numbers separated by colons, for example, 00:01:23:43:45:67.
8. From the **Interface** menu, select the interface to which the MAC address must be applied.
9. Click the **Add** button.

   The MAC Address is added to the Static MAC Address table and to the MAC Address Table.

Remove a Static MAC Address

➢ **To remove a static MAC address:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

The System Information page displays.

5. Select **Switching > Address Table > Address Table > Advanced > Static MAC Address**.

   The Static MAC Address page displays.

6. In the Static MAC Address table, select the check box for the MAC address.

   In the previous figure, none is shown.

7. Click the **Delete** button.

   The MAC address is removed from the Static MAC Address table and from the MAC Address Table.

Configure Routing

4

This chapter contains the following sections.

- *IP Routing Overview*
- *Configure IP Settings*
- *Configure VLAN Routing*
- *Manage IPv4 Routes*
- *Configure Address Resolution Protocol*
- *Configure IPv6*

IP Routing Overview

The switch supports IP routing. When a packet enters the switch, the destination MAC address is checked to see if it matches any of the configured routing interfaces. If it does, the switch searches the host table for a matching destination IP address. If an entry is found, the packet is routed to the host. If no matching entry is found, the switch performs a longest prefix match on the destination IP address. If an entry is found, the packet is routed to the next hop. If no match is found, the packet is routed to the next hop specified in the default route. If no default route exists, the packet is handled appropriately by the switch.

The routing table can include static entries that were manually added. The host table can include static entries that were manually added and entries that were dynamically added through ARP.

Configure IP Settings

From the **Routing > IP** menu, you can access pages that are described in the following sections:

- *Configure the Routing Settings* on page 157
- *View the IP Statistics* on page 158

Configure the Routing Settings

Use the IP Configuration page to configure routing settings for the switch.

➢ **To enable routing 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 *Access the Switch* 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 **Routing > IP > IP Configuration**.

   The IP Configuration page displays.

6. Select the Routing Mode **Enable** radio button.

You must enable the routing mode before the switch can route through any of its interfaces. If you enable the routing mode, routing becomes also possible for VLAN interfaces. The default value is Enable.

7. In the **IPv4 MTU** field, enter the maximum transmission unit (MTU) for IPv4 packets.

   The MTU for IPv4 packets can range from 576 to 9000. The default is 1500.

8. Click the **Apply** button.

   Your settings are saved.

The following table describes the IP configuration information displayed on the page.

Table 44. Global IP status information

Field	Description
Default Time to Live	The default value inserted into the Time-To-Live field of the IP header of datagrams originated by the switch, if a TTL value is not supplied by the transport layer protocol. The default value is 64.
Maximum Next Hops	The maximum number of hops supported by the switch. This is a compile-time constant. The default value is 1.

View the IP Statistics

The statistics reported on this page are as specified in RFC 1213.

➢ **To view 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 *Access the Switch* 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 **Routing > IP > Statistics**.

   The IP Statistics page displays.

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

Table 45. IP Statistics information

Field	Description
IpInReceives	The total number of input datagrams received from interfaces, including those received in error.
IpInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
IpInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
IpForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities that do not act as IP gateways, this counter includes only those packets that were source-routed through this entity, and the source-route option processing was successful.
IpInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
IpInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but that were discarded (for lack of buffer space). This counter does not include any datagrams discarded while awaiting re-assembly.
IpInDelivers	The total number of input datagrams successfully delivered to IP user protocols (including ICMP).
IpOutRequests	The total number of IP datagrams that local IP user protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in ipForwDatagrams.
IpOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that were discarded for reasons such as lack of buffer space. This counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
IpOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in ipForwDatagrams that meet this no-route criterion. This includes any datagrams that a host cannot route because all of its default gateways are down.
IpReasmTimeout	The maximum number of seconds for which received fragments are held while they are awaiting reassembly at this entity.
IpReasmReqds	The number of IP fragments received that were reassembled at this entity.

Table 45. IP Statistics information (continued)

Field	Description
IpReasmOKs	The number of IP datagrams successfully reassembled.
IpReasmFails	The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so on). This is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.
IpFragOKs	The number of IP datagrams that were fragmented at this entity.
IpFragFails	The number of IP datagrams that were discarded because they needed to be fragmented at this entity but could not be, for reasons such as their Don't Fragment flag was set.
IpFragCreates	The number of IP datagram fragments that were generated as a result of fragmentation at this entity.
IpRoutingDiscards	The number of routing entries that were discarded even though they were valid. One possible reason for discarding such an entry could be to free up buffer space for other routing entries.
IcmpInMsgs	The total number of ICMP messages that the entity received. This counter includes all those counted by icmpInErrors.
IcmpInErrors	The number of ICMP messages that the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so on).
IcmpInDestUnreachs	The number of ICMP destination unreachable messages received.
IcmpInTimeExcds	The number of ICMP time exceeded messages received.
IcmpInParmProbs	The number of ICMP parameter problem messages received.
IcmpInSrcQuenchs	The number of ICMP source quench messages received.
IcmpInRedirects	The number of ICMP redirect messages received.
IcmpInEchos	The number of ICMP echo (request) messages received.
IcmpInEchoReps	The number of ICMP echo reply messages received.
IcmpInTimestamps	The number of ICMP timestamp (request) messages received.
IcmpInTimestampReps	The number of ICMP timestamp reply messages received.
IcmpInAddrMasks	The number of ICMP address mask request messages received.
IcmpInAddrMaskReps	The number of ICMP address mask reply messages received.
IcmpOutMsgs	The total number of ICMP messages that this entity attempted to send. This counter includes all those counted by icmpOutErrors.
IcmpOutErrors	The number of ICMP messages that this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value does not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there might be no types of error that contribute to this counter's value.

Table 45. IP Statistics information (continued)

Field	Description
IcmpOutDestUnreachs	The number of ICMP destination unreachable messages sent.
IcmpOutTimeExcds	The number of ICMP time exceeded messages sent.
IcmpOutParmProbs	The number of ICMP parameter problem messages sent.
IcmpOutSrcQuenchs	The number of ICMP source quench messages sent.
IcmpOutRedirects	The number of ICMP redirect messages sent. For a host, this is always zero, since hosts do not send redirects.
IcmpOutEchos	The number of ICMP echo (request) messages sent.
IcmpOutEchoReps	The number of ICMP echo reply messages sent.
IcmpOutTimestamps	The number of ICMP timestamp (request) messages.
IcmpOutTimestampReps	The number of ICMP timestamp reply messages sent.
IcmpOutAddrMasks	The number of ICMP address mask request messages sent.

Configure VLAN Routing

You can configure the switch with some ports supporting VLANs and some supporting routing. You can also configure the switch to allow traffic on a VLAN to be treated as if the VLAN were a router port.

When a port is enabled for bridging (the default) rather than routing, all normal bridge processing is performed for an inbound packet, which is then associated with a VLAN. Its MAC destination address (MAC DA) and VLAN ID are used to search the MAC address table. If routing is enabled for the VLAN, and the MAC DA of an inbound unicast packet is that of the internal bridge-router interface, the packet is routed. An inbound multicast packet is forwarded to all ports in the VLAN, plus the internal bridge-router interface, if it was received on a routed VLAN.

Because a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. VLAN routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when additional segmentation or security is required. This section shows how to configure the switch to support VLAN routing.

From the **Routing > VLAN** menu, you can access pages that are described in the following sections:

- *Use the VLAN Static Routing Wizard* on page 162
- *VLAN Routing Configuration* on page 163

Use the VLAN Static Routing Wizard

The VLAN Routing Wizard lets you create a VLAN routing interface, configure the IP address and subnet mask for the interface, and add ports or LAGs to the VLAN. With this wizard, you can do the following:

- Create a VLAN.
- Add ports to a newly created VLAN.
- Remove selected ports from the default VLAN.
- Enable tagging on a selected port if the port is in another VLAN. Disable tagging if the selected port does not exist in another VLAN.
- Add LAGs to a newly created VLAN.
- Remove selected LAGs from the default VLAN.
- Enable tagging on a selected LAG if the LAG is in another VLAN. Disable tagging if the selected LAG does not exist in another VLAN.
- Enable routing on the VLAN using the IP address and subnet mask entered.

➢ **To use the VLAN Static Routing Wizard:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* 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 **Routing > VLAN > VLAN Routing Wizard**.

   The VLAN Routing Wizard page displays.

6. In the **VLAN ID** field, specify the VLAN ID that is associated with the VLAN.

   The range of the VLAN ID is 1 to 4093.

7. In the **IP Address** field, define the IP address of the VLAN interface.
8. In the **Network Mask** field, define the subnet mask of the VLAN interface.
9. In the Ports table, click each port once, twice, or three times to configure one of the following modes or reset the port to the default settings:
   - **T (Tagged)**. Select the ports on which all frames transmitted for this VLAN are tagged. The ports that are selected are included in the VLAN.

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

By default, the selection is blank, which means that the port is excluded from the VLAN but can be dynamically registered (autodetected) in the VLAN through GVRP.

10. In the LAG table, click each LAG once, twice, or three times to configure one of the following modes or reset the LAG to the default settings:
    - **T (Tagged)**. Select the LAGs on which all frames transmitted for this VLAN are tagged. The LAGs that are selected are included in the VLAN.
    - **U (Untagged)**. Select the LAGs on which all frames transmitted for this VLAN are untagged. The LAGs that are selected are included in the VLAN.

    By default, the selection is blank, which means that the LAG is excluded from the VLAN but can be dynamically registered (autodetected) in the VLAN through GVRP.
11. Click the **Apply** button.

    Your settings are saved.

VLAN Routing Configuration

➢ **To configure VLAN routing:**

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

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

   If you do not know the IP address of the switch, see *Access the Switch* 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 **Routing > VLAN > VLAN Routing Configuration**.

   The VLAN Routing Configuration page displays.
6. From the **VLAN ID** menu, select the VLAN.

   This menu displays the IDs of all VLANs that are configured on the switch.
7. In the **IP Address** field, enter the IP address to be configured for the VLAN routing interface.
8. In the **Subnet Mask** field, enter the subnet mask to be configured for the VLAN routing interface.
9. Click the **Add** button.

The VLAN routing interface is added for the selected VLAN.

The MAC Address field displays the MAC address that is associated with the VLAN routing interface.

Manage IPv4 Routes

The routing table collects routes from multiple sources: static routes and local routes. The routing table can learn multiple routes to the same destination from multiple sources. The routing table lists all routes.

➢ **To configure a basic route and view the table with learned routers:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

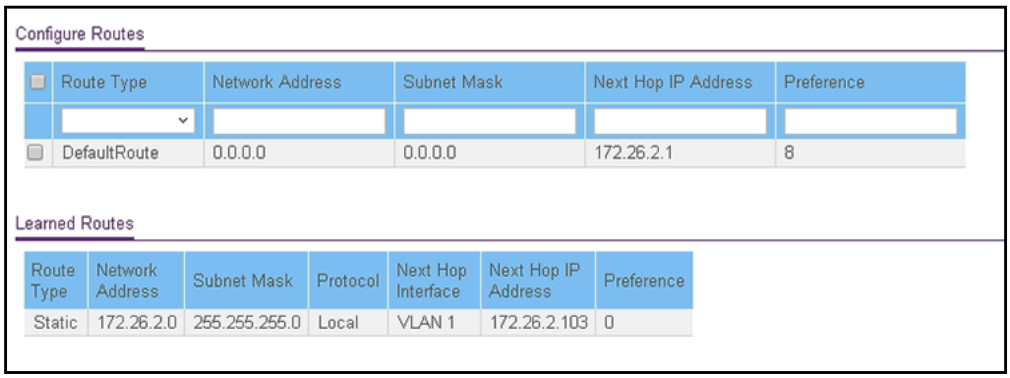
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Routing > Routing Table > Route Configuration**.



6. From the **Route Type** menu, select one of the following route types:
   - **Default**. Creates a default route. You must specify the next hop address and preference.
   - **Static**. Creates a static route. You must specify the network address, subnet mask, next hop address, and preference.

7. Depending on the type of route that you are creating, specify the following information:
   a. In the **Network Address** field, specify the IP address for the destination.
   b. In the **Subnet Mask** field, specify the subnet mask for the attached network.
   c. In the **Next Hop IP Address** field, specify the outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

      The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

   d. In the **Preference** field, specify the preference (sometimes called *administrative distance*), which is an integer value from 1 to 255.

      You can specify the preference value (sometimes called administrative distance) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you control whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.
8. Click the **Add** button.

   The static route is added to the switch.
9. To refresh the page with the latest information about the switch, click the **Refresh** button.

The following table describes the nonconfigurable information that is displayed.

Table 46. Learned Routes information

Field	Description
Route Type	The type of route: Static or Dynamic, depending on how the route was added.
Network Address	The IP address for the destination.
Subnet Mask	The subnet mask for the destination.
Protocol	This field states which protocol created the specified route. The possibilities are one of the following: • Local • Static
Next Hop Interface	The outgoing router interface to use when forwarding traffic to the destination.
Next Hop Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.
Preference	The preference value for the configured next hop.

Configure Address Resolution Protocol

The Address Resolution Protocol (ARP) associates a Layer 2 MAC address with a Layer 3 IPv4 address. The switch supports both dynamic and manual ARP configurations. With manual ARP configuration, you can statically add entries into the ARP table.

ARP is a necessary part of the Internet Protocol (IP) and is used to translate an IP address to a media (MAC) address, defined by a local area network (LAN) such as Ethernet. A station that must send an IP packet must learn the MAC address of the IP destination, or of the next hop router if the destination is not on the same subnet. This is achieved by broadcasting an ARP request packet, to which the intended recipient responds by unicasting an ARP reply containing its MAC address. Once learned, the MAC address is used in the destination address field of the Layer 2 header prepended to the IP packet.

The ARP cache is a table maintained locally in each station on a network. The switch learns ARP cache entries by examining the source information in the ARP packet payload fields, regardless of whether it is an ARP request or response. Thus, when an ARP request is broadcast to all stations on a LAN segment or virtual LAN (VLAN), each recipient can store the sender's IP and MAC address in its respective ARP cache. The ARP response, being unicast, is normally seen only by the requestor, who stores the sender information in its ARP cache. Newer information always replaces existing content in the ARP cache.

Devices can be moved in a network, which means that the IP address that was at one time associated with a certain MAC address is now found using a different MAC, or it disappeared from the network altogether (for example, it was reconfigured, disconnected, or powered off). This leads to stale information in the ARP cache unless entries are updated in reaction to new information seen on the network, periodically refreshed to determine if an address still exists, or removed from the cache if the entry was identified as a sender of an ARP packet during the course of an ageout interval, usually specified through configuration.

The switch supports 512 ARP entries. These entries include dynamic and static ARP entries.

From the **Routing > ARP > Advanced** menu, you can access pages that are described in the following sections:

- *Display the ARP Cache* on page 167
- *Add an Entry to the ARP Table* on page 168
- *Configure the Global Aging-Out Time for ARP* on page 169
- *Remove an ARP Entry From the ARP Cache* on page 170

Display the ARP Cache

You can display ARP entries in the ARP cache based on the remote connections most recently detected switch.

➢ **To display ARP entries in the ARP cache:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* 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 **Routing > ARP > Basic > ARP Cache**.

   The ARP Cache page displays.

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

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

Table 47. ARP cache information

Field	Description
Interface	The routing interface associated with the ARP entry.
IP Address	The IP address of the device (on a subnet) that is attached an existing routing interface of the switch.
MAC Address	The unicast MAC address of the attached device. The address is six two-digit hexadecimal numbers separated by colons, for example, 00:06:29:32:81:40.
Type	The type of ARP entry. Possible values are as follows: • **Static**. An ARP entry that was manually configured. • **Dynamic**. An ARP entry that was learned by the router.

Add an Entry to the ARP Table

You can add an entry to the Address Resolution Protocol (ARP) table.

➢ **To add an entry to the ARP 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 *Access the Switch* 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 **Routing > ARP > Advanced > ARP Create**.

   The Static ARP Configuration page displays. The page also shows the Routing VLAN ARP Cache section.

6. In the **IP Address** field, specify the IP address.

   This must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.

7. In the **MAC Address** field, specify the unicast MAC address of the device.

   Enter the address as six 2-digit hexadecimal numbers separated by colons, for example, 00:06:29:32:81:40.

8. Click the **Add** button.

   The static ARP entry is added to the switch.

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

Table 48. Routing VLANs ARP Cache information

Field	Description
Interface	The routing interface associated with the ARP entry.
IP Address	The IP address of the device (on a subnet) that is attached an existing routing interface of the switch.

Table 48. Routing VLANs ARP Cache information (continued)

Field	Description
MAC Address	The unicast MAC address of the attached device. The address is six two-digit hexadecimal numbers separated by colons, for example, 00:06:29:32:81:40.
Type	The type of ARP entry. Possible values are as follows: • **Static**. An ARP entry that was manually configured. • **Dynamic**. An ARP entry that was learned by the router.

Configure the Global Aging-Out Time for ARP

You can change the global aging-out time for the ARP table. The aging-out time is the period after which an entry in the ARP is automatically deleted.

➢ **To configure the global aging-out time for the ARP 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 *Access the Switch* 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 **Routing > ARP > Advanced > Global ARP Configuration**.

   The Global ARP Configuration page displays.

6. In the **Age Time (secs)** field, enter the time, in seconds, that a dynamic ARP entry remains in the ARP table before aging out.

   The range is 15 to 21600 seconds. The default value is 1200 seconds.

7. Click the **Apply** button.

   Your settings are saved.

Remove an ARP Entry From the ARP Cache

You can remove all or specific entries from the ARP table.

➢ **To remove entries from the ARP 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 *Access the Switch* 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 **Routing > ARP > Advanced > ARP Entry Management**.

   The ARP Entry Management page displays.

6. From the **Remove From Table** menu, select the type of ARP entry to be deleted:
   - **All Dynamic Entries**
   - **All Static Entries**
   - **All Entries**
   - **Specific Entry**. Lets you specify the IP address to be removed.
7. If you select **Specific Entry**, in the **Remove IP Address** field, enter the IP address to be removed.
8. Click the **Apply** button.

   Your settings are saved.

Configure IPv6

IPv6 is supported only on VLAN interfaces, not on physical ports.

From the **Routing > IPv6 > Advanced** menu, you can access pages that are described in the following sections:

- *Configure IPv6 Global Settings* on page 171
- *Add a Static IPv6 Route* on page 172
- *View the IPv6 Route Table* on page 175
- *Configure IPv6 VLAN Interface Settings* on page 176
- *Add an IPv6 Global Address to an IPv6 VLAN* on page 178
- *Add an IPv6 Prefix for Advertisement on an IPv6 VLAN* on page 181
- *View IPv6 Statistics for an Interface* on page 184
- *View or Clear the IPv6 Neighbor Table* on page 186

Configure IPv6 Global Settings

You can configure IPv6 routing parameters for the switch, as opposed to for an interface.

➢ **To configure IPv6 global 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 *Access the Switch* 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 **Routing > IPv6 > Basic > Global Configuration**.

   The IPv6 Global Configuration page displays.

6. Next to IPv6 Unicast Routing, select the **Enable** radio button to globally enable IPv6 unicast routing.

   By default, the Disable radio button is selected.

7. In the **IPv6 Hop Limit** field, enter a value for the unicast hop count used in IPv6 packets originated by the node.

The value is also included in router advertisements. The valid values for hops are 1 to 255, inclusive. The default is 64.

8. In the **ICMPv6 Rate Limit Error Interval** field, specify the number of ICMP error packets allowed per burst interval.

   This value controls the ICMPv6 error packets. The default rate limit is 100 packets per second, meaning that the burst interval is 1000 mseconds. To disable ICMP rate limiting, set this field to 0. The valid rate interval must be in the range 0 to 2147483647 mseconds.

9. In the **ICMPv6 Rate Limit Burst Size** field, specify the number of ICMP error packets allowed per burst interval.

   This value controls the ICMP error packets. The default burst size is 100 packets. When the burst interval is 0, then configuring this field is not a valid operation. The valid burst size is 1 to 200.

10. In the **IPv6 MTU** field, enter the maximum transmission unit (MTU) for IPv6 packets.

    The MTU for IPv6 packets can range from 1280 to 9000. The default is 1500.

11. Click the **Apply** button.

    Your settings are saved.

Add a Static IPv6 Route

➢ **To add a static IPv6 route:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

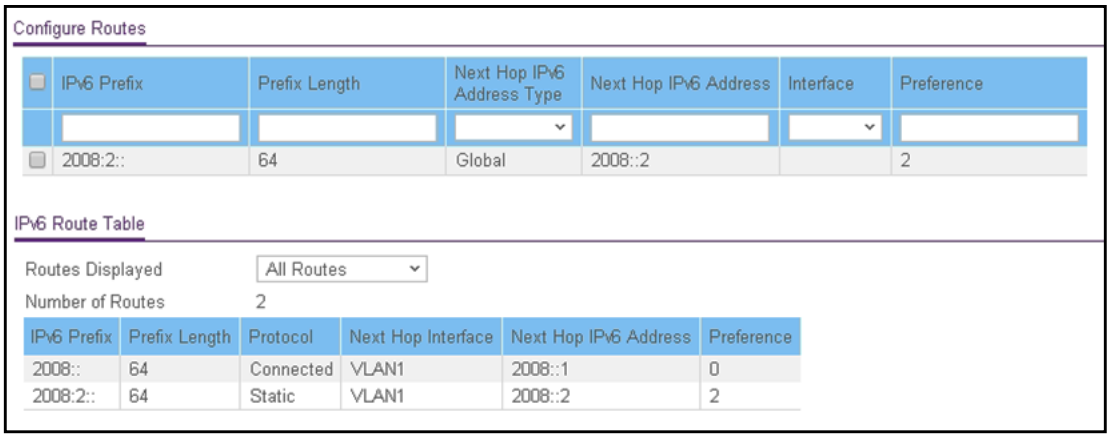
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Routing > IPv6 > Basic > Route Table**.



6. In the **IPv6 Prefix** field, specify the IPv6 network prefix for the destination.
7. In the **Prefix Length** field, specify the IPv6 prefix length for the destination.
8. In the **Next Hop IPv6 Address Type** menu, select one of the following types of IPv6 address for the next hop router:
   - **Link Local**. A link-local IPv6 address over a specified interface. With this selection, you must select an interface from the **Interface** menu.
   - **Global**. A global IPv6 address. With this selection, the **Interface** menu becomes unavailable.
9. In the **Next Hop IPv6 Address** field, specify the outgoing router IPv6 address to use when forwarding traffic to the next router (if any) in the path toward the destination.

   The next router is always one of the adjacent neighbors or the IPv6 address of the local interface for a directly attached network.
10. In the **Interface** menu, select the outgoing IPv6 routing VLAN interface that must be used to forward traffic to the destination.

    Selecting an interface applies only when the selection in the **Next Hop IPv6 Address Type** menu is **Link Local**.
11. In the **Preference** field, specify the router preference.
12. Click the **Add** button.

    The route is added to the switch.

Change the Preference for a Static IPv6 Route

➢ **To change the preference for a static IPv6 route:**

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

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

If you do not know the IP address of the switch, see *Access the Switch* 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 **Routing > IPv6 > Basic > Route Table**.

   The Configure Routes page displays. The page also shows the IPv6 Route Table.

6. In the table in the Configure Routes section, select the check box for the static IPv6 route.
7. In the **Preference** field, specify another router preference.
8. Click the **Apply** button.

   Your settings are saved.

Remove a Static IPv6 Route

➢ **To remove one or more static IPv6 routes:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* 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 **Routing > IPv6 > Basic > Route Table**.

   The Configure Routes page displays. The page also shows the IPv6 Route Table.

6. In the table in the Configure Routes section, select the check boxes for the static IPv6 routes.
7. Click the **Delete** button.

   The routes are removed from the switch.

View the IPv6 Route Table

The IPv6 Route Table contains IPv6 routes that were statically added, IPv6 routes that were discovered through the Neighbor Discovery (ND) protocol, and IPv6 routes that were derived from manually added IPV6 addresses.

➢ **To view the IPv6 Route 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 *Access the Switch* on page 12.

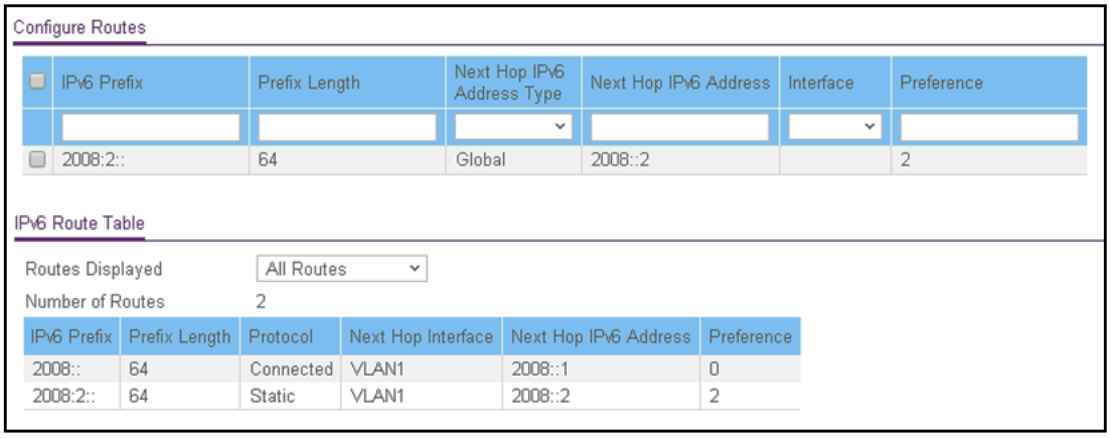
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Routing > IPv6 > Basic > Route Table**.



6. To specify which type of routes to display in the IPv6 Route Table, from the **Routes Displayed** menu, select one of the following options:
   - **All Routes**. Show all active IPv6 routes.
   - **All Static Routes**. Show only the manually configured routes.
7. To refresh the page with the latest information about the switch, click the **Refresh** button.

The following table describes the nonconfigurable data that is displayed.

Table 49. IPv6 Route Table information

Field	Description
Number of Routes	The total number of active routes in the route table.
IPv6 Prefix	The network prefix for the active route.
Prefix Length	The prefix length for the active route.
Protocol	The type of protocol for the active route: • **Static**. The route was manually defined. • **ND (Neighbor Discovery)**. The route was discovered through the ND protocol. • **Connected**. The route was derived from a manually configured IPv6 address.
Next Hop Interface	The interface over which the route is active. For a rejected route, the next hop would be a *Null0* interface.
Next Hop IP Address	The next hop IPv6 address for the active route.
Preference	The route preference of the configured route.

Configure IPv6 VLAN Interface Settings

➢ **Configure IPv6 VLAN 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.

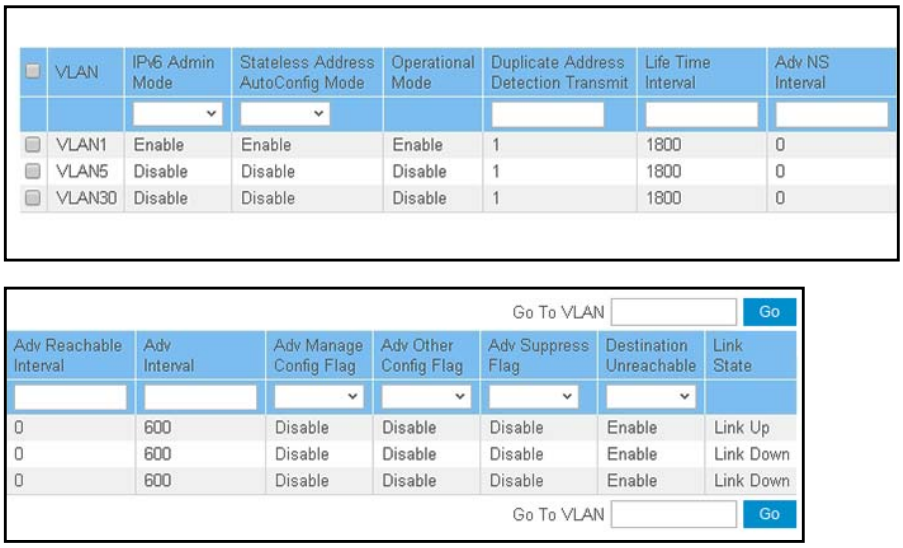
   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   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 **Routing > IPv6 > Advanced > VLAN Configuration**.

The page is very wide and is therefore shown in the following two figures.



	VLAN	IPv6 Admin Mode	Stateless Address AutoConfig Mode	Operational Mode	Duplicate Address Detection Transmit	Life Time Interval	Adv NS Interval
	VLAN1	Enable	Enable	Enable	1	1800	0
	VLAN5	Disable	Disable	Disable	1	1800	0
	VLAN30	Disable	Disable	Disable	1	1800	0

Go To VLAN Go

Adv Reachable Interval	Adv Interval	Adv Manage Config Flag	Adv Other Config Flag	Adv Suppress Flag	Destination Unreachable	Link State
0	600	Disable	Disable	Disable	Enable	Link Up
0	600	Disable	Disable	Disable	Enable	Link Down
0	600	Disable	Disable	Disable	Enable	Link Down

Go To VLAN Go

6. To view more columns, move the gray bar below the table to the right.
7. Select one or more VLANs by taking one of the following actions:
   - To configure a single VLAN, select the check box associated with the VLAN, or, in the **Go To VLAN** field, type the VLAN in the format VLANxx in which xx is the VLAN ID, and click the **Go** button. (VLANxxx in which xxx is the VLAND ID and VLANxxxx in which xxxx is the VLAN ID are also valid search entries.)
   - To configure multiple VLANs with the same settings, select the check box associated with each VLAN.
   - To configure all VLANs with the same settings, select the check box in the heading row.
8. From the **IPv6 Admin Mode** menu, select **Enable** or **Disable**.

   When IPv6 mode is enabled, the VLAN is capable of IPv6 operation. The default value is Disable.
9. From the **Stateless Address AutoConfig Mode** menu, select to enable or disable the stateless address autoconfiguration mode.

   The default value is Disable.
10. In the **Duplicate Address Detection Transmits** field, specify the number of duplicate address detection (DAD) transmits.

    The DAD transmits value must be in the range 0 to 600. The default is 1.
11. In the **Life Time Interval** field, specify the router advertisement life time interval that is sent from the VLAN.

    This value must be greater than or equal to the maximum advertisement interval. 0 means do not use the router as the default router. The range of router life time is 0 to 9000. The default is 1800.

12. In the **Adv NS Interval** field, specify the retransmission time of router advertisements that are sent from the VLAN.

    A value of 0 means the interval is not specified for the router. The range of the neighbor solicit interval is 1000 to 4294967295. The default is 0.

13. In the **Adv Reachable Interval** field, specify the router advertisement time.

    This is the time allocated to consider the neighbors reachable after ND confirmation. The range of reachable time is 0 to 3600000. The default is 0.

14. In the **Adv Interval** field, specify the maximum time that is allowed between outgoing router advertisements from the VLAN.

    The range of the maximum advertisement interval is 4 to 1800. The default value is 600.

15. From the **Adv Managed Config Flag** menu, specify the setting for the router advertisement managed address configuration flag.

    When you select **Enable**, end nodes use DHCPv6. When you select **Disable**, end nodes autoconfigure addresses. The default value is Disable.

16. From the **Adv Other Config Flag** menu, select to enable or disable the router advertisement other stateful configuration flag.

    The default value is Disable.

17. From the **Adv Suppress Flag** menu, select to enable or disable the router advertisement suppression on the VLAN.

    The default value is Disable.

18. From the **Destination Unreachables** menu, select to enable or disable the mode for sending ICMPv6 destination unreachable messages from the VLAN.

    If this mode is disabled, the VLAN does not send ICMPv6 destination unreachable messages. By default, the IPv6 destination unreachables mode is enabled.

19. Click the **Apply** button.

    Your settings are saved.

The following table describes the nonconfigurable data that is displayed.

Table 50. IPv6 VLAN Configuration information

Field	Description
Operational Mode	The operational mode of the VLAN (Enable or Disable).
Link State	The state of the link (Link Up or LInk Down).

Add an IPv6 Global Address to an IPv6 VLAN

IPv6 link-local addresses are created automatically when you enable the IPv6 admin mode on an VLAN interface, and they cannot be removed or edited. However, you can manually configure IPv6 global addresses on a VLAN.

➢ **To add an IPv6 global address to an IPv6 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 *Access the Switch* on page 12.

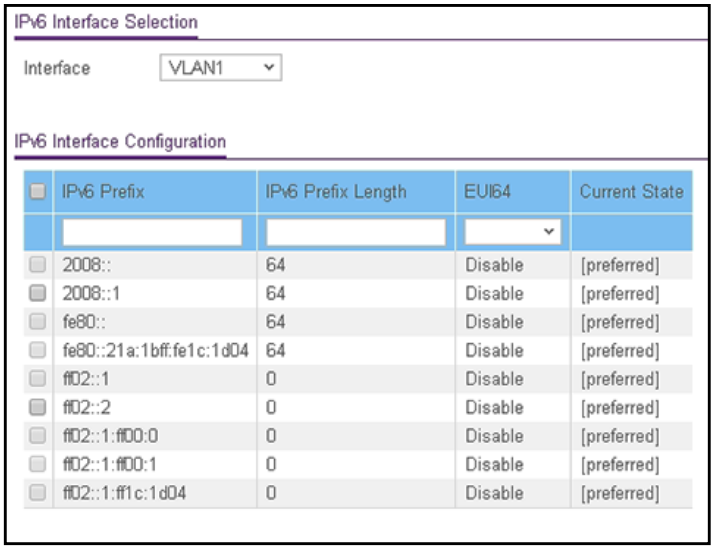
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Routing > IPv6 > Advanced > IPv6 Addresses**.



   The table contains both IPv6 link-local addresses and IPv6 global addresses that were manually added to the IPv6 VLAN.

6. From the **Interface** menu, select the VLAN.
7. For the **IPv6 Prefix** field and the **Prefix Length** field, either select the check box for a preconfigured IPv6 address, or specify a new IPv6 address by entering an IPv6 prefix and prefix length in the global address format.
8. From the **EUI64** menu, select **Enable** or **Disable** to indicate whether the specified 64-bit unicast prefix is enabled.

   The default value is Disable.

9. Click the **Add** button.

   The IPv6 address is added to the VLAN.

The Current State field is a nonconfigurable field that shows the state of the IPv6 address. The state can be one of the following:

- **Tent**. Routing is disabled or the address does not work because of a duplicate address detection (DAD) condition.
- **Active**. The IPv6 address is valid and active.
- **Preferred**. The IPv6 address was verified to be unique, valid, and active.

Change the Settings for an IPv6 Global Address on an IPv6 VLAN

IPv6 link-local addresses are created automatically when you enable the IPv6 admin mode on an VLAN interface, and they cannot be changed. However, you can change the settings for an IPv6 global address that you added on a VLAN.

➢ **To change the settings for an IPv6 global address on an IPv6 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 *Access the Switch* 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 **Routing > IPv6 > Advanced > IPv6 Addresses**.

   The IPv6 Interface Selection page displays. The page also shows the IPv6 Interface Configuration table.
6. From the **Interface** menu, select the VLAN.
7. Select the check box for the IPv6 global address.

   You cannot select a check box for an IPv6 link-local address.

   The settings display in the fields in the table heading.
8. Change the settings as needed.
9. Click the **Apply** button.

   Your settings are saved.

Remove an IPv6 Global Address From an IPv6 VLAN

IPv6 link-local addresses are created automatically when you enable the IPv6 admin mode on an VLAN interface, and they cannot be removed or edited. However, you can manually remove one or more IPv6 global addresses from a VLAN.

➢ **To remove one or more IPv6 global addresses from an IPv6 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 *Access the Switch* 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 **Routing > IPv6 > Advanced > IPv6 Addresses**.

   The IPv6 Interface Selection page displays. The page also shows the IPv6 Interface Configuration table.

6. From the **Interface** menu, select the VLAN.
7. Select the check boxes for the IPv6 global addresses.

   You cannot select any check boxes for IPv6 link-local addresses.

8. Click the **Delete** button.

   The IPv6 global addresses are removed from the IPv6 VLAN.

Add an IPv6 Prefix for Advertisement on an IPv6 VLAN

When you add an IPv6 prefix for advertisement on an IPv6 VLAN, the prefix is advertised on all interfaces that are members of the VLAN.

➢ **To add an IPv6 prefix for advertisement on an IPv6 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 *Access the Switch* on page 12.

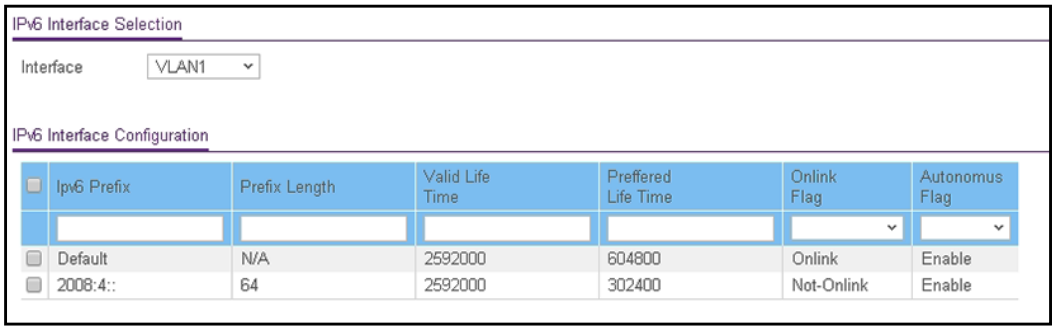
The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Routing > IPv6 > Advanced > Prefix Configuration**.



6. From the **Interface** menu, select the VLAN.
7. In the **Ipv6 Prefix** field, specify the IPv6 prefix.
8. In the **Prefix Length** field, specify the IPv6 prefix length.
9. In the **Valid Life Time** field, specify the router advertisement per prefix time.

   This is the time during which the switch considers the prefix valid for on-link determination. The valid life time must be in the range 0 to 4294967295. The default value is 2592000.

10. In the **Preferred Life Time** field, specify the router advertisement per prefix time.

    An autoconfigured address generated from this prefix is preferred. The preferred life time must be in the range 0 to 4294967295. The default value is 604800.

11. From the **Onlink Flag** menu, select one of the following options:
    - **Onlink**. The prefix can be used for on-link determination. The default is Onlink.
    - **No-Onlink**. The prefix cannot be used for on-link determination.
    - **Off-Link**. The prefix can be inserted in the routing table.
12. From the **Autonomous Flag** menu, select **Enable** or **Disable** to specify whether the selected prefix can be used for autonomous address configuration.

    The default value is Enable.

13. Click the **Add** button.

    The IPv6 address prefix is added to the VLAN.

Change the Settings for an IPv6 Prefix for Advertisement on an IPv6 VLAN

You can change the settings for a prefix for advertisement on an IPv6 VLAN.

➢ **To change the settings for an IPv6 prefix for advertisement on an IPv6 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 *Access the Switch* 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 **Routing > IPv6 > Advanced > Prefix Configuration**.

   The IPv6 Interface Selection page displays. The page also shows the IPv6 Interface Configuration table.
6. From the **Interface** menu, select the VLAN.
7. Select the check box for the IPv6 prefix.

   The settings display in the fields in the table heading.
8. Change the settings as needed.
9. Click the **Apply** button.

   Your settings are saved.

Remove an IPv6 Prefix From an IPv6 VLAN

You can remove one or more IPv6 prefixes from an IPv6 VLAN. You cannot remove the default IPv6 prefix.

➢ **To remove one or more IPv6 prefixes from an IPv6 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 *Access the Switch* 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 **Routing > IPv6 > Advanced > Prefix Configuration**.

   The IPv6 Interface Selection page displays. The page also shows the IPv6 Interface Configuration table.

6. From the **Interface** menu, select the VLAN.
7. Select the check boxes for the IPv6 prefixes.
8. Click the **Delete** button.

   The IPv6 prefixes are removed from the IPv6 VLAN.

View IPv6 Statistics for an Interface

➢ **To view IPv6 statistics 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 *Access the Switch* 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 **Routing > IPv6 > Advanced > Statistics**.

   The IPv6 Interface Statistics page displays.

6. From the **Interface** menu, select the interface.

   When you select an interface, the page refreshes and all fields are updated.

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

The following table describes the nonconfigurable IPv6 statistics that are displayed.

Table 51. IPv6 Statistics information

Field	Description
Total Datagrams Received	The total number of input datagrams received by the interface, including those received in error.
Received Datagrams Locally Delivered	The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed, which might not be the input interface for some of the datagrams.
Received Datagrams Discarded Due To Header Errors	The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, and so on.
Received Datagrams Discarded Due To MTU	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
Received Datagrams Discarded Due To No Route	The number of input datagrams discarded because no route could be found to transmit them to their destination.
Received Datagrams With Unknown Protocol	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed, which might not be the input interface for some of the datagrams.
Received Datagrams Discarded Due To Invalid Address	The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, ::0) and unsupported addresses (such as addresses with unallocated prefixes). For entities that are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Received Datagrams Discarded Due To Truncated Data	The number of input datagrams discarded because datagram frame didn't carry enough data.
Received Datagrams Discarded Other	The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but that were discarded for reasons such as lack of buffer space. This counter does not include any datagrams discarded while awaiting reassembly.
Received Datagrams Reassembly Required	The number of IPv6 fragments received that needed to be reassembled at this interface. This counter is incremented at the interface to which these fragments were addressed, which might not be the input interface for some of the fragments.
Datagrams Successfully Reassembled	The number of IPv6 datagrams successfully reassembled. This counter is incremented at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the fragments.

Table 51. IPv6 Statistics information (continued)

Field	Description
Datagrams Failed To Reassemble	The number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, and so on). This is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed, which might not be the input interface for some of the fragments.
Datagrams Forwarded	The number of output datagrams that this entity received and forwarded to their final destinations. In entities that do not act as IPv6 routers, this counter includes only those packets that were source-routed through this entity, and the source-route processing was successful. For a successfully forwarded datagram the counter of the outgoing interface is incremented.

View or Clear the IPv6 Neighbor Table

➢ **To view or clear the IPv6 Neighbor Table:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* 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 **Routing > IPv6 > Advanced > Neighbor Table**.

   The IPv6 Neighbor Table displays.

6. Use the **Search** menu and field to search for IPv6 routes by IPv6 address or interface number:
   - **Search by IPv6 address**. Select **IPv6 Address** from the **Search** menu. Enter the 128-byte hexadecimal IPv6 address in four-digit groups separated by colons, for example, 2001:231F:::1. Then click the **Go** button.

     If the address exists, the entry is displayed. An exact match is required.
   - **Search by Interface**. Select **Interface** from the **Search** menu. Enter the interface using the respective naming convention (for example, xg1 or l1). Then click the **Go** button.

If the address exists, the entry is displayed.

7. To clear the IPv6 neighbors for all interfaces, click the **Clear** button.
8. To refresh the page with the latest information about the switch, click the **Refresh** button.

The following table describes the nonconfigurable data that is displayed.

Table 52. IPv6 Neighbor Table information

Field	Description
Interface	The interface whose settings are displayed in the current table row.
IPv6 Address	The IPv6 address of the neighbor or interface.
MAC Address	The MAC address associated with an interface.
isRtr	Indicates whether the neighbor is a router. If the neighbor is a router, the value is True. If the neighbor is not a router, the value is False.
Neighbor State	The state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache: • **Incomplete**. Address resolution is being performed on the entry. A neighbor solicitation message was sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message is not yet received. • **Reachable**. Positive confirmation was received within the last Reachable Time milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent. • **Stale**. More than Reachable Time milliseconds elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent. • **Delay**. More than Reachable Time milliseconds elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE. • **Probe**. Seeks a reachability confirmation by resending neighbor solicitation messages every Retrans Timer milliseconds until a reachability confirmation is received.
Last Updated	Time since the address was confirmed to be reachable.

Configure Quality of Service

5

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

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.

This chapter covers the following topics:

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

Manage Class of Service

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

Eight queues per port are supported.

From the **QoS > CoS > Advanced** menu, you can access pages that are described in the following sections:

- *CoS Configuration* on page 189
- *Configure Global CoS Settings* on page 190
- *Configure CoS Interface Settings for an Interface* on page 190
- *Configure the Global CoS Queue Settings* on page 192
- *Configure the Global 802.1p to Queue Mapping* on page 193
- *DSCP to Queue Mapping* on page 194

CoS Configuration

Use the CoS Configuration page to set the class of service trust mode of an interface. Each port in the switch can be configured to trust one of the packet fields (802.1p or IP DSCP), or to not trust any packet's priority designation (untrusted mode). If the port is set to a trusted mode, it uses a mapping table appropriate for the trusted field being used. This mapping table indicates the CoS queue to which the packet 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > CoS > Basic > CoS Configuration**.

   The CoS Configuration page displays.

6. 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. This QoS setting lets you map traffic with one of 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. This QoS setting lets you map traffic with particular DSCP bits to one of multiple queues.
7. Click the **Apply** button.

   Your settings are saved.

Configure CoS Interface Settings for an Interface

Use the CoS Interface Configuration page to configure the interface shaping rate and interface ingress rate limit to one or more interfaces.

➢ **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 *Access the Switch* on page 12.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > CoS > Advanced > CoS Interface Configuration**.

   The CoS Interface Configuration page displays.

6. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
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 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.

   The Interface Trust Mode column display the globally configured trust mode (see *Configure Global CoS Settings* on page 190). This mode is the same for all interfaces.
8. The **Interface Trust Mode** field displays whether the selected interfaces trust a particular packet marking when the packet enters the port. The data for all the ports is taken from the Global Trust Mode. To set this for a specific port, select one of the following values:
   - **Untrusted**. Do not trust any CoS packet marking at ingress.
   - **802.1p**. The eight priority tags that are specified in IEEE 802.1p are p0 to p7. The QoS setting lets you map each of the eight priority levels to one of four internal hardware priority queues.This is the default setting.
   - **DSCP.** The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP) bits.
9. In the **Interface Shaping Rate** field, specify the maximum bandwidth allowed.

   This specification is typically used to shape the outbound transmission rate in this range of 64–10000000 Kbps. The shaping rate (Kb) value is the value of the interface shaping rate configured. The default value is 0. The value 0 means that the maximum is unlimited.
10. In the **Interface Ingress Rate Limit** field, specify the ingress rate allowed.

    The range is 100 to 10000000 Kbps. The default value is 0. The value 0 means that the maximum is unlimited.
11. Click the **Apply** button.

    Your settings are saved.

Configure the Global CoS Queue Settings

Use the Queue Configuration page to define what a particular queue does by configuring switch egress queues. You can control the amount of bandwidth that is used by the queue and the scheduling of packet transmission from the set of all queues on a port.

You can configure eight queues as strict priority, weighted round robin (WRR) priority, or a combination of both. If a specific queue is configured as WRR, all the queues with a lower number are also WRR queues.

The configuration process is simplified by allowing each CoS queue parameter to be configured globally. A global configuration change is automatically applied to all ports.

➢ **To configure the global CoS queue 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 *Access the Switch* on page 12.

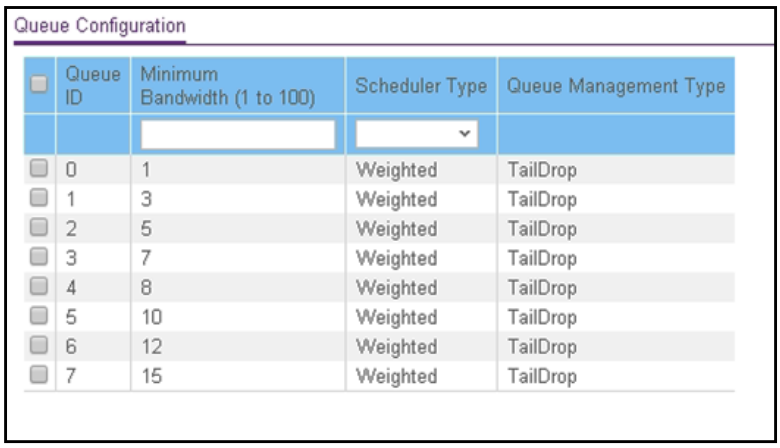
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > CoS > Advanced > Interface Queue Configuration**.



6. Select the check box for the queue that you want to configure.

   You can select more than one check box or you can select the check box in the table heading to configure all queues in the same way.

7. In the **Minimum Bandwidth** field, specify the minimum guaranteed bandwidth allotted to the queue.

   Enter a value in the range of 1 to 100 that reflects the relative bandwidth of this queue. The bandwidth allocation per queue is the configured weight divided by the sum of all the configured weights. The sum of the minimum bandwidths for all queues does not need to equal 100.

   This setting is configurable and applicable only if the selection from the **Scheduler Type** menu is **Weighted**.

8. From the **Scheduler Type** menu, select one of the following options:
   - **Weighted**. Weighted round robin (WRR) associates a weight to each queue. This is the default setting.
   - **Strict**. Strict lets the switch service traffic with the highest priority on a queue first.

   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. All packets on a queue are normally processed unless congestion occurs. If congestion occurs, any additional packets that are queued are dropped.

9. Click the **Apply** button.

   Your settings are saved.

Configure the Global 802.1p to Queue Mapping

You can view or change which internal traffic classes are mapped to the 802.1p priority class values in Ethernet frames that the switch receives. The priority-to-traffic class mappings can be applied globally only. 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 *Access the Switch* on page 12.

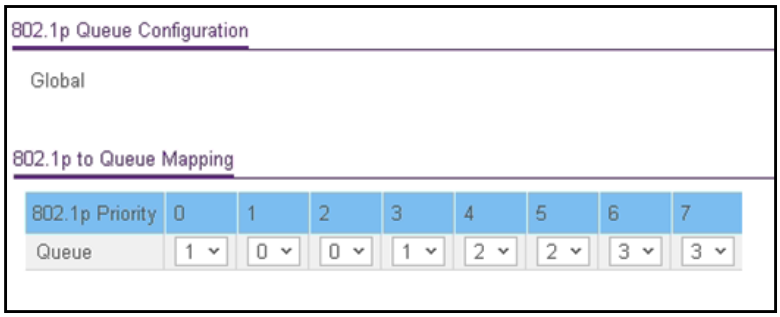
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > CoS > Advanced > 802.1p to Queue Mapping**.



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

   The 802.1p Priority row contains traffic class selectors for each of the eight 802.1p priorities to be mapped. The priority goes from low (0) to high (7). For example, traffic with a priority of 0 is for most data traffic and is sent using best effort. Traffic with a higher priority, such as 7, might be time-sensitive traffic, such as voice or video.

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

7. Click the **Apply** button.

   Your settings are saved.

DSCP to Queue Mapping

Use the DSCP to Queue Mapping page to map an internal traffic class to a DSCP value.

The allowed Per Hop Behavior (PHBs) values, apart from other DSCP experimental values, are as follows:

- **Class Selector (CS) PHB**. These values are based on IP precedence.
- **Assured Forwarding (AF) PHB**. These values are used to define four main levels that allow the switch to sort and manipulate certain 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 must handle excess traffic and an application requires a bandwidth guarantee, the EF traffic must receive this rate independently of other traffic that attempts to transit the switch.
- **Other DSCP Values (Local/Experimental Use)**. These are less common values.

➢ **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.

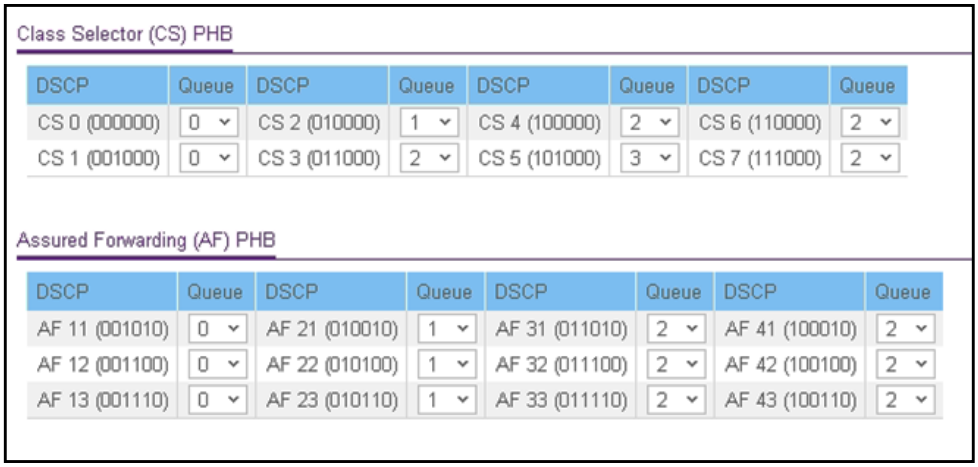
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **QoS > CoS > Advanced > DSCP to Queue Mapping**.



   The previous figure does not show the Expedited Forwarding (EF) PHB values and the Other DSCP Values (Local/Experimental Use) values.
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.
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 are designed to provide best effort data delivery service. Best effort service implies that the network attempts to deliver the data in a timely fashion. During times of congestion, packets might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email and file transfer, a slight degradation in service is

acceptable and in many cases unnoticeable. Conversely, any degradation of service can negatively affect applications with strict timing requirements, such as voice or multimedia.

From the **QoS > Diffserv > Advanced** menu, you can access pages that are described in the following sections:

- *DiffServ Overview* on page 196
- *View the Global DiffServ Resources* on page 197
- *Specify DSCP Remark Values for Violate Action IP Packets* on page 197
- *Configure IPv4 DiffServ Classes* on page 199
- *Configure an IPv6 DiffServ IPv6 Classes* on page 203
- *Configure a DiffServ Policy* on page 207
- *Configure DiffServ Service Interfaces* on page 212
- *View DiffServ Service Statistics* on page 213

DiffServ Overview

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.

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 class 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. 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.

View the Global DiffServ Resources

By default, the DiffServ administrative mode is enabled. (You cannot manually disable it.) You can view the used DiffServ resources.

➢ **To view the global DiffServ resources:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > DiffServ > Basic > DiffServ Configuration**.

   The Diffserv Configuration page displays.

   The Diffserv Used Resources field displays the number of configured DiffServ classes on the switch. The maximum number of available system resources, including DiffServ classes, is 2048. For more information about system resources, see *View the System Resource Utilization* on page 309.

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

Specify DSCP Remark Values for Violate Action IP Packets

If you assign a policer to a class map (which represents a traffic flow), you can specify the action that must be taken when the amount of traffic in the flow exceeds the specified limits. This action is referred to as the violate action and applies to the portion of the traffic that causes the flow to exceed its QoS limit. That portion of the traffic is referred to as the violate action IP packets.

When this action occurs, the switch remaps the original DSCP value of the violate action IP packets with a new value based on the information in the DSCP Violate Action Mapping table. The switch uses the new values to assign resources and the egress queues to these packets. The switch also physically replaces the original DSCP value in the violate action packets with the new DSCP value.

This feature changes (remarks) the DSCP tags for incoming traffic switched between trusted QoS domains.

For example, assume three levels of service—A, B, and C—and that the DSCP incoming values used to mark these levels are 10, 20, and 30 respectively. If this traffic is forwarded to

another service provider that provides the same three levels of service, but uses DSCP values 16, 24, and 48, the DSCP violate action mapping changes the incoming values as they are mapped to the outgoing values.

➢ **To specify the DSCP remark values for violate action IP 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 *Access the Switch* on page 12.

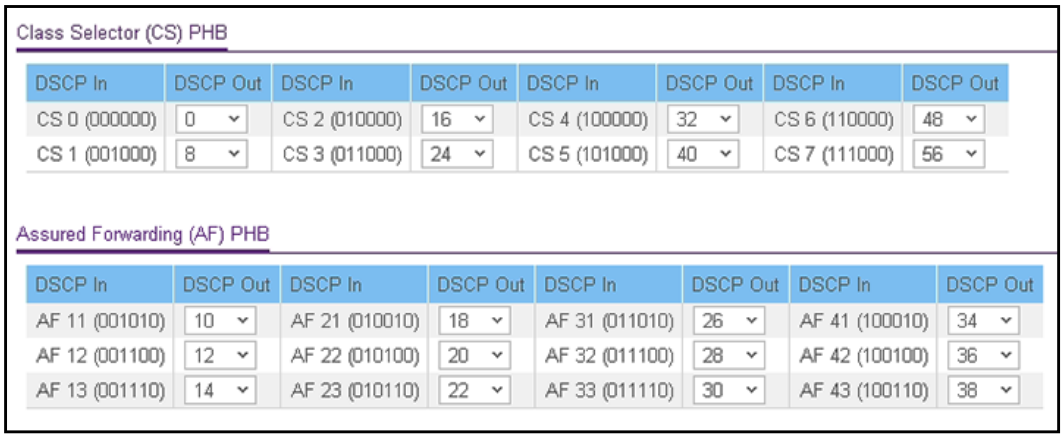
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > DiffServ > Basic > DSCP Violate Action Mapping**.



   The previous figure does not show the Expedited Forwarding (EF) PHB values and the Other DSCP Values (Local/Experimental Use) values.

6. For each DSCP value, from the corresponding **DSCP Out** menu, select to which internal traffic class the DSCP value must be remarked.

   The original DSCP value for the incoming traffic is shown in the DSCP In field.

7. Click the **Apply** button.

   Your settings are saved.

Configure IPv4 DiffServ Classes

You can add a DiffServ class and define the criteria that are associated 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 as described in the following procedure.

Add and Configure an IPv4 DiffServ Class

➢ **To add and configure an IPv4 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > DiffServ > Advanced > Class Configuration**.

   The Class Configuration page displays.

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

   The Class Name field also lists all the existing IPv4 DiffServ class names, from which one can be selected for modification or deletion.

7. From the **Class Type** menu, select the class type **All**.

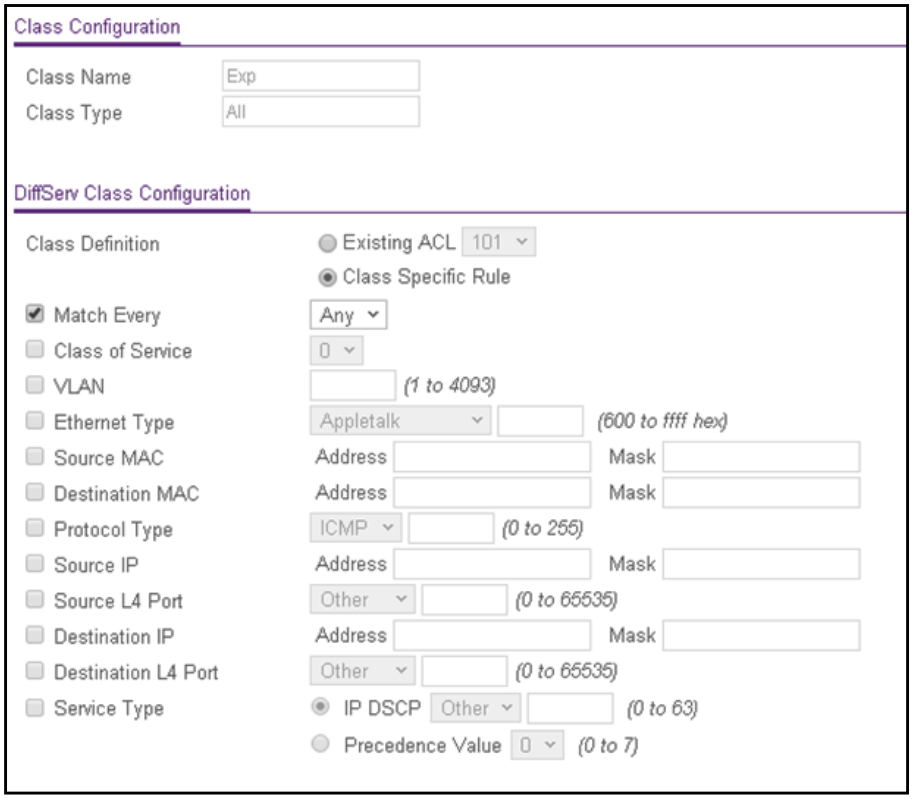
   The switch supports only the class type value **All**, which means that all the various match criteria defined for the class are satisfied for a packet match. **All** signifies the logical AND statement of all the match criteria.

8. Click the **Add** button.

   The new class is added.

9. After creating the class, click the class name.

The class name is a hyperlink to the page on which you can define the class configuration.



The class name and class type are stated in the Class Configuration section at the top of the page. These fields are nonconfigurable on this page.

10. Select one of the following Class Definition radio buttons:
    - **Existing ACL**. From the menu, select an existing ACL for traffic classification. For information about creating ACLs, see *Configure Access Control Lists* on page 258. If you select this radio button, the fields on the page are disabled and you cannot define classification rules.
    - **Class Specific Rule**. Use class-specific rules. If you select this radio button (which is selected by default), the fields on the page are enabled so that you can define classification rules. See the next step.
11. If you select the **Class Specific Rule** radio button, define the criteria that must be associated with the DiffServ class:
    - **Match Every**. Select this check box to add a match condition that considers all packets to belong to the class. The only selection from the **Match Every** menu is **Any**. If you select the **Match Every** check box, you cannot define any other options.
    - **Class of Service**. Select this check box to require the Class of Service (CoS) value in an Ethernet frame header to match the specified CoS value. This option lists all the values for the Class of Service match criterion in the range 0 to 7 from which one can be selected.

- **VLAN**. Select this check box to require a packet's VLAN ID to match a VLAN ID or a VLAN ID within a continuous range. If you configure a range, a match occurs if a packet's VLAN ID is the same as any VLAN ID within the range. The VLAN value is in the range of 0–4093.
- **Ethernet Type**. Select this check box to require the EtherType value in the Ethernet frame header to match the specified EtherType value. After you select the check box, select the EtherType keyword from the menu of common protocols that are mapped to their Ethertype value. If you select **User Value** from the menu, you can enter a value in the field next to the menu.
- **Source MAC**. Select this check box to require a packet's source MAC address to match the specified MAC address. After you select this check box, use the following fields to configure the source MAC address match criteria:
  - **Address**. The source MAC address to match.
  - **Mask**. The MAC mask, which specifies the bits in the source MAC address to compare against the Ethernet frame. Use Fs and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.
- **Destination MAC**. Select this check box to require a packet's destination MAC address to match the specified MAC address. After you select the check box, use the following fields to configure the destination MAC address match criteria:
  - **Address**. The destination MAC address to match.
  - **Mask**. The MAC mask, which specifies the bits in the destination MAC address to compare against an Ethernet frame. Use Fs and zeros to configure the MAC mask. An F means that the bit is checked, and a zero in a bit position means that the data is not significant. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is ff:ff:00:00:00:00, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). Note that this is not a wildcard mask, which ACLs use.
- **Protocol Type**. Select this check box to require a packet's Layer 4 protocol to match the specified protocol, which you must select from the menu. If you select **Other** from the menu, you can enter a protocol number from 0 to 255.
- **Source IP**. Select this check box to require a packet's source IP address to match the specified IP address. After you select the check box, use the following fields to configure the source IP address match criteria:
  - **Address**. The source IP address format to match in dotted-decimal format.
  - **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 check box to require a packet's TCP/UDP source port to match the specified protocol, which you must select from the menu. If you select **Other** from the menu, you can enter a source port number.

- **Destination IP**. Select this check box to require a packet's destination IP address to match the specified IP address. After you select the check box, use the following fields to configure the destination IP address match criteria:
  - **Address**. The destination IP address format to match in dotted-decimal format.
  - **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 check box to require a packet's TCP/UDP destination port to match the specified protocol, which you must select from the menu. If you select **Other** from the menu, you can enter a destination port number.
- **Service Type**. Select this check box either to require the packet's IP DiffServ Code Point (DSCP) value to match the specified IP DSCP keyword code or to require the packet's IP precedence value to match the specified number from 0 to 7:
  - **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. If you select **Other** from the menu, you can 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.

12. Click the **Apply** button.

    Your settings are saved.

Change the Criteria for an Existing IPv4 DiffServ Class

➢ **To change the criteria for an existing IPv4 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > DiffServ > Advanced > Class Configuration**.

   The Class Configuration 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 an IPv4 DiffServ Class

➢ **To delete an IPv4 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > DiffServ > Advanced > Class Configuration**.

   The Class Configuration page displays.

6. Select the check box for the class name.
7. Click the **Delete** button.

   The class is removed.

Configure an IPv6 DiffServ IPv6 Classes

The IPv6 class configuration feature extends the existing QoS ACL and DiffServ functionality by providing support for IPv6 packet classification. An Ethernet IPv6 packet is distinguished from an IPv4 packet by its unique Ethertype value, so all IPv6 classifiers include the Ethertype field. An IPv6 access list serves the same purpose as its IPv4 counterpart.

The destination and source IPv6 addresses use a prefix length value instead of an individual mask to qualify them as a subnet addresses or a host addresses. The flow label is a 20-bit number that is unique to an IPv6 packet, used by end stations to signify some form of Quality of Service (QoS) handling in routers.

Packets that match an IPv6 classifier are allowed to be marked using only the 802.1p (CoS) field or the IP DSCP field in the Traffic Class octet. IP precedence is not defined for IPv6. This is not an appropriate type of packet marking.

IPv6 ACL/DiffServ assignment is appropriate for LAG interfaces. The procedures described by an ACL or DiffServ policy are equally applicable on a LAG interface.

Add and Configure an IPv6 DiffServ Class

➢ **To add and configure an IPv6 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

   The IPv6 Class Name a page displays.

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

   The Class Name field also lists all the existing IPv6 DiffServ class names, from which one can be selected for modification or deletion.

7. From the **Class Type** menu, select the class type **All**.

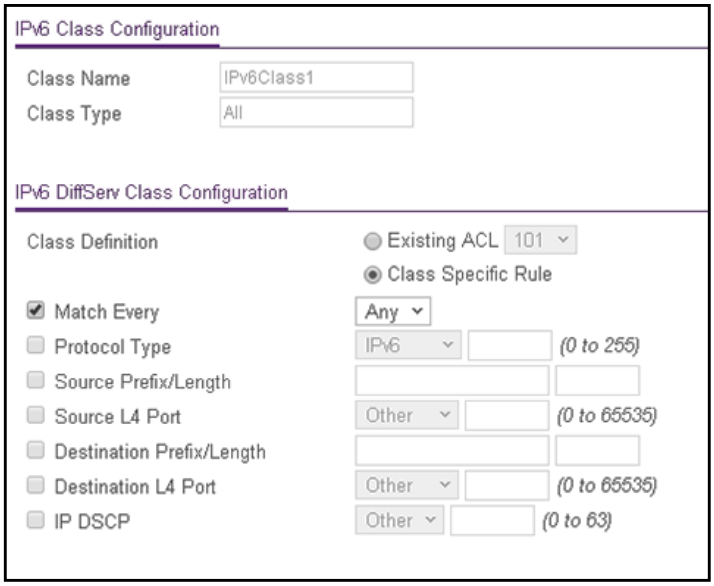
   The switch supports only the class type value **All**, which means that all the various match criteria defined for the class are satisfied for a packet match. **All** signifies the logical AND statement of all the match criteria.

8. Click the **Add** button.

   The new class is added.

9. After creating the class, click the class name.

The class name is a hyperlink to the page on which you can define the class configuration.



The class name and class type are stated in the IPv6 Class Configuration section at the top of the page. These fields are nonconfigurable on this page.

10. Select one of the following Class Definition radio buttons:
    - **Existing ACL**. From the menu, select an existing ACL for traffic classification. For information about creating ACLs, see *Configure Access Control Lists* on page 258. If you select this radio button, the fields on the page are disabled and you cannot define classification rules.
    - **Class Specific Rule**. Use class-specific rules. If you select this radio button (which is selected by default), the fields on the page are enabled so that you can define classification rules. See the next step.
11. If you select the **Class Specific Rule** radio button, define the criteria that must be associated with the IPv6 DiffServ class:
    - **Match Every**. Select this check box to add a match condition that considers all packets to belong to the class. The only selection from the **Match Every** menu is **Any**.

      Note: If you select the **Match Every** check box, you cannot define any other options.

    - **Protocol Type**. Select this check box to require a packet's Layer 4 protocol to match the specified protocol, which you must select from the menu. If you select **Other** from the menu, you can enter a protocol number from 0 to 255.
    - **Source Prefix/Length**. Select this check box to require a packet's source prefix and prefix length to match the specified source IPv6 prefix and prefix length. The prefix must always be specified with the prefix length. The prefix can be in the hexadecimal range from 0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF and the prefix length can be in the range from 0 to 128.

- **Source L4 Port**. Select this check box to require a packet's TCP/UDP source port to match the specified protocol, which you must select from the menu. If you select **Other** from the menu, you can enter a source port number.
- **Destination Prefix/Length**. Select this check box to require a packet's destination prefix and prefix length to match the specified source IPv6 prefix and prefix length. The prefix must always be specified with the prefix length. The prefix can be in the hexadecimal range from 0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF and the prefix length can be in the range from 0 to 128.
- **Destination L4 Port**. Select this check box to require a packet's TCP/UDP destination port to match the specified protocol, which you must select from the menu. If you select **Other** from the menu, you can enter a destination port number.
- **IP DSCP**. Select this check box 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. If you select **Other** from the menu, you can 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.

12. Click the **Apply** button.

    Your settings are saved.

Change the Criteria for an Existing IPv6 DiffServ Class

➢ **To change the criteria for an existing IPv6 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

   The IPv6 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 an IPv6 DiffServ Class

➢ **To delete an IPv6 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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

   The IPv6 Class Name page displays.
6. Select the check box for the class name.
7. Click the **Delete** button.

   The class is removed.

Configure a DiffServ Policy

Use the Policy Configuration page to associate a collection of classes with one or more policies.

Add and Configure a DiffServ Policy

➢ **To add 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 *Access the Switch* on page 12.

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

The default password is **password**.

The System Information page displays.

5. Select **QoS > DiffServ > Advanced > Policy Configuration**.

   The Policy Configuration page displays.

6. Enter a policy name in the **Policy Name** field.

   You cannot specify the policy type. By default, the policy type is In, indicating that the policy applies to ingress packets.

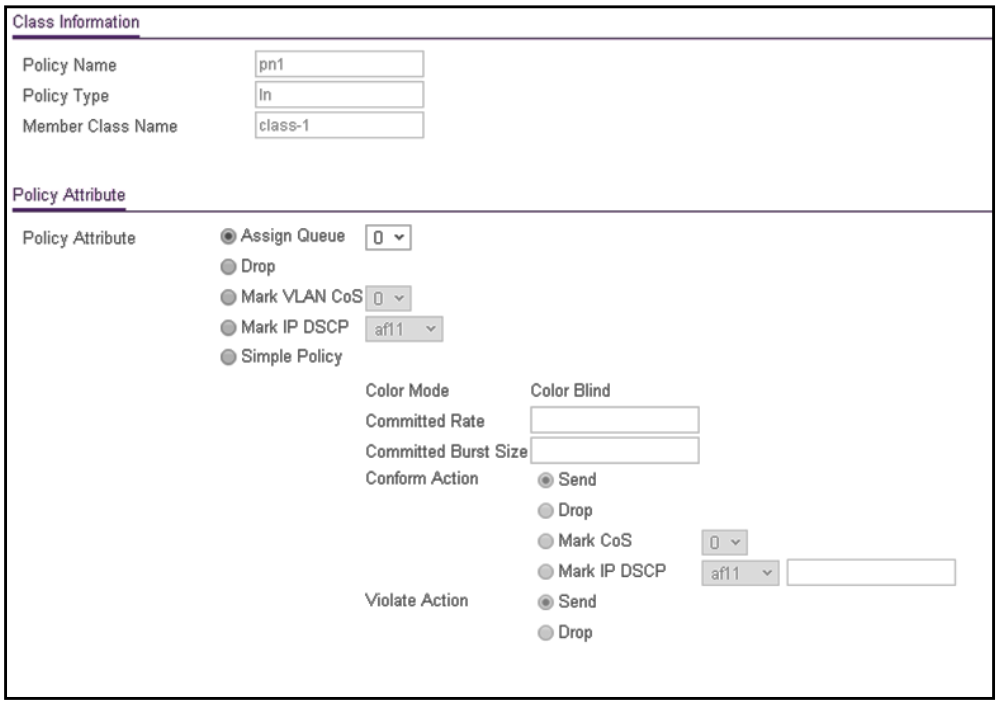
7. From the **Member Class** menu, optionally select an existing class that you want to associate with the new policy.
8. Click the **Add** button.

   The new policy is added.

9. After creating the policy, click the policy name.

   The policy name is a hyperlink to the page on which you can define the policy attributes.

   Note: The hyperlink is available only if the class associated with the policy was configured using class-specific rules. If the class was configured using an existing ACL, the hyperlink is not available because only the ACL rules of permit or deny apply and policy attributes are not applicable.



The policy name, policy type, and member class name are stated in the Class Information section at the top of the page. These fields are nonconfigurable on this page.

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

    This is a value in the range from 0 to 7.

11. Configure the policy attributes:
    - **Drop**. Select this radio button to require each inbound packet to be dropped.
    - **Mark VLAN CoS**. Select this radio button to specify the VLAN priority, which you must select from the menu. The VLAN priority is expressed as an integer value in the range from 0 to 7.
    - **Mark IP DSCP**. Select this radio button to require packets to be marked with an IP DSCP keyword code, which you must select from the menu. If you select **Other** from the menu, you can enter an IP DSCP value from 0 to 63. The DSCP value is defined as the high-order 6 bits of the Service Type octet in the IP header.
    - **Simple Policy**. Select this radio button to define the traffic policing style for the class. A simple policy uses a single data rate and burst size, resulting in one of two outcomes: conform or violate. You must define the policy as described in the next step.

12. If you select the **Simple Policy** radio button, you can specify the traffic policing style for the class:
    - **Color Mode**. The default color mode is Color Blind. Color classes do not apply.
    - **Committed Rate**. Enter the committed rate that is applied to conforming packets by specifying a value in the range from 1 to 4294967295 Kbps.
    - **Committed Burst Size**. Enter the committed burst size that is applied to conforming packets by specifying an integer from 3000 to 19173960. The committed burst size is the maximum amount of traffic that is allowed in one burst (in bytes).

    Note: The switch uses the token bucket algorithm, in which the committed rate is the rate at which the bucket is filled, and the committed burst size is the size of the bucket. This means that the committed burst size is the maximum size of a burst that the switch can send.

13. If you select the **Simple Policy** radio button, you can select the conforming and violating actions.

    The Conform Action section and Violate Action section list the actions to be taken on conforming packets according to the policing metrics. By default, both conforming packets and violating packets are sent.

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

    - **Send**. Packets are forwarded unmodified. This is the default conforming action and the default violating action.
    - **Drop**. Packets are dropped. This action can apply to a conforming action and to a 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.

  This action can apply only to a conforming action.

- **Mark IP DSCP**. Packets are marked by DiffServ with the specified DSCP value before being forwarded. This selection requires that the DSCP field is set. You must select a DSCP code from the menu. If you select **Other** from the menu, you can 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.

  This action can apply only to a conforming action.

14. 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > DiffServ > Advanced > Policy Configuration**.

   The Policy Configuration page displays.

6. Click the policy name, which is a hyperlink.

   The page on which you can change the policy attributes displays.

7. Change the policy attributes as needed.
8. Click the **Apply** button.

   Your settings are saved.

Assign Another Class to an Existing DiffServ Policy

➢ **To assign another class to 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > DiffServ > Advanced > Policy Configuration**.

   The Policy Configuration page displays.

6. Select the check box for the policy name.
7. From the **Member Class** menu, select another class.
8. Click the **Apply** button.

   Your settings are saved.

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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **QoS > DiffServ > Advanced > Policy Configuration**.

   The Policy Configuration page displays.

6. Select the check box for the policy name.
7. Click the **Delete** button.

   The policy is removed.

Configure DiffServ Service Interfaces

You can assign a policy to one or more interfaces.

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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **QoS > DiffServ > Advanced > Service Configuration**.

   The Service Configuration page displays.
6. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
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 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.
8. From the **Policy Name** menu, select a policy name.
9. Click the **Apply** button.

   Your settings are saved.

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

Table 53. Service Interface Configuration information

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

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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **QoS > DiffServ > Advanced > Service Configuration**.

   The Service Interface Configuration page displays.
6. Select the check boxes that are associated with the interfaces from which you want to remove the policy.
7. From the **Policy In Name** menu, select **None**.
8. Click the **Apply** button.

   Your settings are saved.

View DiffServ Service Statistics

You can display service-level statistical information about all interfaces to which DiffServ policies are attached.

➢ **To view the DiffServ service statistics:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **QoS > DiffServ > Advanced > Service Statistics**.

   The Service Statistics page displays.
6. Click the **Refresh** button to refresh the page with the latest information about the switch.

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

Table 54. DiffServ Service Statistics information

Field	Description
Interface	List of all valid slot number and port number combinations on the switch with a DiffServ policy currently attached in the inbound direction.
Direction	List of the traffic direction of interface as In. Shows only the directions for which a DiffServ policy is currently attached.
Policy Name	Name of the policy currently attached to the specified interface and direction.
Operational Status	Shows the operational status of this service interface, which is always Up.
Member Classes	All DiffServ classes currently defined as members of the selected policy name.

Manage Device Security

6

This chapter covers the following topics:

- *Management Security Settings*
- *Configure Management Access*
- *Configure Port Authentication*
- *Set Up Traffic Control*
- *Configure Access Control Lists*

Management Security Settings

From the **Management Security** menu, you can access the pages that are described in the following sections:

- *Change the Password* on page 216
- *Reset the Password to the Factory Default Value* on page 217
- *Configure RADIUS Servers* on page 218
- *Configure TACACS+ Servers* on page 224
- *Configure Authentication Lists* on page 227

Change the Password

You can change the login password that is required for access to the switch.

➢ **To change the login password for the web-based management interface:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > User Configuration > Change Password**.

   The Change Password page displays.

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

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

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

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

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

   The entered password is displayed in dots.

9. Click the **Apply** button.

   Your settings are saved.

Reset the Password to the Factory Default Value

You can reset the login password that is required for access to the switch to the factory default value.

➢ **To reset the login password for the web-based management interface:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > User Configuration > Change Password**.

   The Change Password page displays.

6. Select the **Reset Password** check box.
7. Click the **Apply** button.

   The password is reset to the default password, which is **password**.

Note: If you forget the password and are unable to log in to the switch management interface, press the **Factory Defaults** button on the front panel of the switch for more than two seconds. The device reboots, and all switch settings, including the password, are reset to the factory default values. (The **Reset** button only reboots the switch.)

Configure RADIUS Servers

Remote Authorization Dial-In User Service (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)

From the **Security > Management Security > RADIUS** menu, you can access the pages that are described in the following sections:

- *Configure the Global RADIUS Server Settings* on page 218
- *Configure a RADIUS Authentication Server on the Switch* on page 220
- *Add a Primary or Secondary RADIUS Authentication Server to the Switch* on page 220
- *Modify the Settings for a RADIUS Authentication Server on the Switch* on page 221
- *Remove a RADIUS Authentication Server From the Switch* on page 221
- *Configure a RADIUS Accounting Server* on page 222
- *Add a RADIUS Accounting Server to the Switch* on page 222
- *Modify the Settings for a RADIUS Accounting Server on the Switch* on page 223
- *Remove a RADIUS Accounting Server From the Switch* on page 223

Configure the Global RADIUS Server Settings

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

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

➢ **To configure the global RADIUS server settings:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > RADIUS > Global Configuration**.

   The RADIUS Configuration page displays.

   The Current Server IP Address field is blank if no servers are configured (see *Configure a RADIUS Authentication Server on the Switch* on page 220). The switch supports up to eight RADIUS servers. If more than one RADIUS server is configured, the current server is the server configured as the primary server. If no servers are configured as the primary server, the current server is the most recently added RADIUS server.

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

   The valid range is from 1 to 15. The default value is 3.

   Consider the maximum delay time when you are configuring RADIUS maximum retransmit and RADIUS time-out values. See the information in the introduction of this section.

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

   The valid range is from 1 to 30. The default value is 3.

   Consider the maximum delay time when you are configuring RADIUS maximum retransmit and RADIUS time-out values. See the information in the introduction of this section.

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 55. RADIUS Configuration information

Field	Description
Current Server Address	The address of the current server. This field is blank if no servers are configured.
Number of Configuration Servers	The number of configured RADIUS servers. The value can range from 0 to 8.

Configure a RADIUS Authentication Server on the Switch

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

Add a Primary or Secondary RADIUS Authentication Server to the Switch

➢ **To add a primary or secondary RADIUS authentication server to the switch:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > RADIUS > Server Configuration**.

   The Server Configuration page displays.

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 the server uses to verify the RADIUS server authentication.

   The valid 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** for a primary authentication server or **Secondary** for a secondary authentication server.
11. Click the **Add** button.

    The server is added to the switch.

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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > RADIUS > Server Configuration**.

   The Server Configuration page displays.

6. Select the check box for the server.
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 a remove a RADIUS authentication server from the switch:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > RADIUS > Server Configuration**.

   The Server Configuration page displays.

6. Select the check box for the server.
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 configure various settings for a single RADIUS accounting server on the network. RADIUS accounting is supported for both AAA and 802.1x sessions.

Add a RADIUS Accounting Server to the Switch

➢ **To add a RADIUS accounting server to the switch:**

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Security > Management Security > RADIUS > Accounting Server Configuration**.

   The Accounting Server Configuration page displays.
6. In the **Accounting Server Address** field, specify the IP address of the RADIUS accounting server.
7. In the **Port** field, specify the UDP port number the server uses to verify the RADIUS accounting server authentication.

   The valid range is from 1 to 65535. The default value is 1813.
8. From the **Secret Configured** menu, select **Yes** to add a RADIUS secret in the next field.

   You must select **Yes** before you can configure the RADIUS secret. After you add the RADIUS accounting server, this field indicates whether the shared secret for this server was configured.
9. In the **Secret** field, type the shared secret to use with the specified accounting server.
10. From the **Accounting Mode** menu, select **Enable** to enable the RADIUS accounting mode.

11. Click the **Add** button.

    The server is added to the switch.

Modify the Settings for a RADIUS Accounting Server on the Switch

➢ **To modify the settings for a RADIUS accounting server on the switch:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > RADIUS > Accounting Server Configuration**.

   The Accounting Server Configuration page displays.

6. Modify the configuration for the selected accounting server.
7. Click the **Apply** button.

   Your settings are saved.

Remove a RADIUS Accounting Server From the Switch

➢ **To a remove a RADIUS accounting server from the switch:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > RADIUS > Accounting Server Configuration**.

The Accounting Server Configuration page displays.

6. Click the **Delete** button.

   All fields are set to their defaults.

Configure TACACS+ Servers

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.

From the **Security > Management Security > TACACS+** menu, you can access the pages that are described in the following sections:

- *Configure the Global TACACS+ Settings* on page 224
- *Configure a TACACS+ Server on the Switch* on page 225
- *Modify the Settings for a TACACS+ Server on the Switch* on page 226
- *Remove a TACACS+ Server From the Switch* on page 227

Configure the Global TACACS+ Settings

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

➢ **To configure the global TACACS+ settings:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > TACACS+ > TACACS+ Configuration**.

   The ACACS+ Configuration page displays.

6. In the **Key String** field, specify the authentication and encryption key for TACACS+ communications between the switch and the TACACS+ server.

   The valid range is 0–128. 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 1–30 seconds. If you do not specify a value, the switch uses a default value of 5 seconds.

8. Click the **Apply** button.

   Your settings are saved.

Configure a TACACS+ Server on the Switch

Use the TACACS+ Server Configuration page to configure up to five 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > TACACS+ > TACACS+ Server Configuration**.

   The TACACS+ Server Configuration page displays.

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 valid range is 0–65535.

8. In the **Port** field, specify the authentication port value for TACAS+ server sessions. It must be within the range 0–65535. If you do not specify a value, the switch uses the standard TCP port 49 for sessions with the server.
9. In the **Key String** field, specify the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server.

   The valid range is 0–128. The key must match the key used on the TACACS+ server.
10. In the **Connection Timeout** field, specify the time that passes before the connection between the device and the TACACS+ server times out.

    The range is 1–30 seconds. 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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Security > Management Security > TACACS+ > TACACS+ Server Configuration**.

   The TACACS+ Server Configuration page displays.
6. Select the check box for the server.
7. Modify the configuration for the selected accounting server.
8. Click the **Apply** button.

   Your settings are saved.

Remove a TACACS+ Server From the Switch

➢ **To a 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > TACACS+ > TACACS+ Server Configuration**.

   The TACACS+ Server Configuration page displays.

6. Select the check box for the server.
7. Click the **Delete** button.

   The RADIUS accounting server is removed.

Configure Authentication Lists

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

Note: The admin user is assigned to a preconfigured list that is named defaultList and that you cannot delete.

From the **Security > Management Security > Authentication List** menu, you can access the pages that are described in the following sections:

- *Configure an HTTP Authentication List* on page 228
- *Configure an HTTPS Authentication List* on page 229

Configure an HTTP Authentication List

Use the HTTP Authentication List page to 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > Authentication List > HTTP Authentication List**.

   The HTTP Authentication List page displays.

6. Select the check box for 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** or **None**, you cannot configure a second and third method. If you configure another method and then select **Local** or **None** as the first method, no other method is tried. User authentication occurs in the order that the methods are selected. Possible methods are as follows:

   - **Local**. The user's locally stored ID and password are used for authentication. This is the default method. Because the local method does not time out, if you select this option as the first method, no other method is tried, even if you specified more than one method.
   - **RADIUS**. The user's ID and password are authenticated using the RADIUS server. If you select **Radius** or **Tacacs** as the first method and an error occurs during the authentication, the switch uses method 2 to authenticate the user.
   - **TACACS+**. The user's ID and password are authenticated using the TACACS+ server. If you select **Radius** or **Tacacs** as the first method and an error occurs during the authentication, the switch attempts user authentication method 2.
   - **None**. The authentication method is unspecified. If you select this option as the first method, no other method is tried, even if you specified more than one method.

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

Use the HTTPS Authentication List to 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Management Security > Authentication List > HTTPS Authentication List**.

   The HTTPS Authentication List page displays.

6. Select the check box for 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** or **None**, you cannot configure a second and third method. If you configure another method and then select **Local** or **None** as the first method, no other method is tried. User authentication occurs in the order that the methods are selected. Possible methods are as follows:

   - **Local**. The user's locally stored ID and password are used for authentication. This is the default method. Because the Local method does not time out, if you select this

option as the first method, no other method is tried, even if you specified more than one method.

- **RADIUS**. The user's ID and password are authenticated using the RADIUS server. If you select **Radius** or **Tacacs** as the first method and an error occurs during the authentication, the switch uses method 2 to authenticate the user.
- **TACACS+**. The user's ID and password are authenticated using the TACACS+ server. If you select **Radius** or **Tacacs** as the first method and an error occurs during the authentication, the switch attempts user authentication method 2.
- **None**. The authentication method is unspecified. If you select this option as the first method, no other method is tried, even if you specified more than one method.

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 Management Access

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

From the **Security > Management Security > Access** menu, you can access the pages that are described in the following sections:

- *Configure HTTP Settings* on page 231
- *Configure HTTPS Settings* on page 231
- *Manage the Certificate* on page 233
- *Configure Access Control* on page 235

Configure HTTP Settings

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

➢ **To configure the HTTP server settings:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Access > HTTP > HTTP Configuration**.

   The HTTP Configuration page displays.

6. In the **HTTP Session Soft Timeout** field, specify the number of minutes an HTTP session can be idle before a time-out occurs.

   The value must be in the range of 0–60 minutes. The default value is 10 minutes. The currently configured value is shown when the web page is displayed.

   After the session is inactive for the configured time, you are automatically logged out and must reenter the password to access the management interface. A value of zero means that the session does not time out.

7. Click the **Apply** button.

   Your settings are saved.

   The Maximum Number of HTTP Sessions field shows the maximum number of HTTP sessions that can exist at the same time, which is 5 sessions. This number is not configurable.

Configure HTTPS Settings

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

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

➢ **To configure HTTPS settings:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

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

   The HTTPS Configuration page displays.

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

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

7. In the **HTTPS Port** field, enter the HTTPS port number.

   The value must be in the range of 1 to 65535. Port 443 is the default value. The configured value is displayed.

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

   The value must be in the range of 1 to 60 minutes. The default value is 10 minutes.

9. Click the **Apply** button.

   Your settings are saved.

   The Maximum Number of HTTPS Sessions field shows the maximum number of HTTPS sessions that can exist at the same time, which is 2 sessions. This number is not configurable.

Manage the Certificate

Use the Certificate Management page to manage the certificate. The switch can contain a single certificate (or set of certificates.)

Generate a Certificate

➢ **To generate a 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Access > HTTPS > Certificate Management**.

   The Certificate Management page displays. The page also shows the Certificate Generation Status section.

6. Select the **Generate Certificates** radio button.
7. Click the **Apply** button.

   The switch generates a certificate.

   The Certificate Generation Status field shows progress information.

Import a Certificate

➢ **To import a 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 *Access the Switch* on page 12.

   The login window opens.

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

The default password is **password**.

The System Information page displays.

5. Select **Security** > **Access > HTTPS** > **Certificate Management**.

   The Certificate Management page displays.

6. Select the **Import Certificates** radio button.

   Additional fields display.

7. In the **Certificate** field, **Public Key** field, and **Private Key** field respectively, paste the certificate, public key, and private key from an external file.
8. Click the **Apply** button.

   The certificate is imported.

   The Certificate Generation Status field shows progress information.

Generate a Certificate Request

➢ **To generate a certificate request:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security** > **Access > HTTPS** > **Certificate Management**.

   The Certificate Management page displays.

6. Select the **Generate Certificates Request** radio button.

   Additional fields display.

7. Specify applicable information in the **Common Name**, **Organization Unit**, **Organization Name**, **Location**, **State**, and **Country** fields.

   The Certification Request field displays the certification request text that you can use to generate the certificate request.

8. Click the **Generate Request** button.

The certificate request is generated. You can send this request to your certificate authority for signing.

The Certificate Generation Status field shows progress information.

Delete the Certificate

The switch can contain only one certificate (or set of certificates). You can delete this certificate.

➢ **To delete the 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security** > **Access > HTTPS** > **Certificate Management**.

   The Certificate Management page displays.

6. Select the **Delete Certificates** radio button.
7. Click the **Apply** button.

   The certificate is removed.

Configure Access Control

Access control allows you to configure an access control profile and set access rules. Access control defines a single access control list (ACL, but in this case referred to as an access profile) for management packets. This ACL can be composed of one or more access rules.

Creating an access control profile involves the following steps that are described in detail in the sections that are mentioned in the steps:

1. Create an access profile (see *Create an Access Profile* on page 236).
2. Configure access rules for the access profile (see *Add an Access Rule* on page 236).
3. Activate the access profile (see *Activate or Deactivate an Access Control Profile and View the Profile Summary* on page 239).

Create an Access Profile

Use the Access Profile Configuration page to set up a security access profile.

➢ **To configure an access profile:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Access > Access Control > Access Profile Configuration**.

   The Access Profile Configuration page displays. The page also shows the Profile Summary section.

6. In the **Access Profile Name** field, enter a name for the access profile.

   The maximum length is 32 characters.

7. Click the **Apply** button.

   Your settings are saved.

   By default, the new access profile is deactivated, that is, the **Deactivate Profile** radio button is selected. The Profile Summary does not yet display any information for the access profile because you did not yet add any access rules.

Add an Access Rule

After you create an access control profile, you must add on ore more security access rules to the profile.

➢ **To add an access rule for 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 *Access the Switch* on page 12.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Access > Access Control > Access Rule Configuration**.

   The Access Rule Configuration page displays.

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 by traffic that matches the rule criteria. A Deny rule blocks traffic 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 **HTTP, Secure HTTP (SSL)**, and **SNMP**.

8. In the **Source IP Address** field, enter the source IP address of the client originating the management traffic.
9. In the **Mask** field, specify the subnet mask of the client that originates the management traffic.
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 are ignored. For example, if a source IP 10.10.10.10 is configured with priority 1 to permit, and source IP 10.10.10.10 is configured with priority 2 to deny, then access is permitted if the profile is active, and the second rule is ignored.

11. Click the **Add** button.

    The access rule is added.

Change an Access Rule

You can change an access rule only when the associated access profile is in a deactivated state (see *Activate or Deactivate an Access Control Profile and View the Profile Summary* on page 239).

➢ **To change an access rule for 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 *Access the Switch* on page 12.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Access > Access Control > Access Rule Configuration**.

   The Access Rule Configuration page displays.

6. Select the check box for the access rule.

   The settings display in the fields in the table heading.

7. Change the settings as needed.
8. Click the **Apply** button.

   Your settings are saved.

Remove an Access Rule

You can remove an access rule only when the associated access profile is in a deactivated state (see *Activate or Deactivate an Access Control Profile and View the Profile Summary* on page 239).

➢ **To remove one or more access rules for 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Access > Access Control > Access Rule Configuration**.

   The Access Rule Configuration page displays.

6. Select the check boxes for the access rules.
7. Click the **Delete** button.

   The access rules are removed from the access control profile.

Activate or Deactivate an Access Control Profile and View the Profile Summary

After you set up an access profile and add access rules to the profile, you must activate the profile to be able to use it. (You do not need to activate the profile, but if you do not, you cannot use it.)

If you want to make a change to an access rule for an access control profile, you must first deactivate the access control profile.

➢ **To activate or deactivate an access profile and view the profile 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Access > Access Control > Access Profile Configuration**.

   The Access Profile Configuration page displays. The page also shows the Profile Summary section.

6. Take one of the following actions:
   - To activate the access profile, select the **Activate Profile** radio button.
   - To deactivate the access profile, select the **Deactivate Profile** radio button.
7. Click the **Apply** button.

   Your settings are saved.

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

The following table describes the nonconfigurable data that is displayed.

Table 56. Access profile configuration profile summary

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

Table 56. Access profile configuration profile summary (continued)

Field	Description
Mask	The subnet mask of the IP address.
Priority	The priority of the rule.

Remove an Access Control Profile

If you do not want to use an access control profile, you can deactivate it. However, if you no longer need a profile, you can remove it entirely.

➢ **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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Access > Access Control > Access Profile Configuration**.

   The Access Profile Configuration page displays.

6. Select the **Remove Profile** radio button.
7. Click the **Apply** button.

   Your settings are saved.

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 (unless dynamic VLAN assignment is enabled on port, in which case user authentication occurs individually). 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:

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

From the **Security > Management Security > Port Authentication** menu, you can access the pages that are described in the following sections:

- *Configure Global 802.1X Settings* on page 241
- *Manage Port Authentication* on page 243
- *View the Port Summary* on page 245
- *View the Client Summary* on page 247

Configure Global 802.1X Settings

You can configure global 802.1X port access control settings on the switch by enabling port access control on the switch, enabling the guest VLAN (which allows unauthenticated users to gain temporary and limited access to network resources), and enabling the forwarding of EAPoL frames if 802.1x is disabled on the switch.

➢ **To configure the global 802.1X 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

The System Information page displays.

5. Select **Security > Port Authentication > Basic > 802.1X Configuration**.

   The 802.1X Configuration page displays.

6. To enable the 802.1X administrative mode on the switch, select the Port Based Authentication State **Enable** radio button.

   The default value is Disable.

   Note: If 802.1X is enabled, authentication is performed by a RADIUS server. This means that the primary authentication method must be RADIUS. To set the method, select **Security > Management Security > Authentication List** and select **Radius** as method 1 for defaultList. For more information, see *Configure RADIUS Servers* on page 218 and *Configure Authentication Lists* on page 227.

   When port-based authentication is globally disabled, the switch does not check for 802.1X authentication before allowing traffic on any ports, even if the ports are configured to allow only authenticated users.

7. To enable and configure a guest VLAN, do the following:

   a. Select the Guest VLAN **Enable** radio button.

      The default value is Disable. A guest VLAN can allow unauthenticated users to gain temporary and limited access to network resources.

   b. From the **Guest VLAN ID** menu, select the VLAN that must serve as the guest VLAN.

   c. In the **Guest VLAN Period** field, enter the maximum period that access to the guest VLAN is allowed.

      The period can range from 30 to 180 minutes. The default value is 90 minutes.

   Note: For the guest VLAN to become functional, you still must enable the guest VLAN on one or more ports (see *Manage Port Authentication* on page 243).

8. To enable Extensible Authentication Protocol (EAP) over LAN (EAPoL) flood support on the switch, select the EAPOL Flood Mode **Enable** radio button.

   The default value is Disable. If 802.1x is disabled on the switch, EAPoL frames are forwarded.

9. Click the **Apply** button.

   Your settings are saved.

Manage Port Authentication

Use the Port Authentication page to enable and configure port access control on one or more ports.

Configure 802.1X Settings for a Port

➢ **To configure 802.1X settings for a port:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Port Authentication > Advanced > Port Authentication**.

   The Port Authentication page displays.

6. To view more columns, move the horizontal scroll bar below the table.
7. Select the check box for 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 system automatically detects the mode of the port.
     - **Authorized**. The system places the port into an authorized state without being authenticated. The port sends and receives normal traffic without client port-based authentication.
     - **Unauthorized**. The system denies the selected port system access by moving the interface into unauthorized state. The switch cannot provide authentication services to the client through the port.
     - **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.

- **Dynamic VLAN Assignment**. From the menu, select **Enable** to enable dynamic VLAN assignment on the port. By default, dynamic VLAN assignment is disabled on all ports.

  This feature is also known as RADIUS Assigned VLAN Attribute (RAVA). If this feature is enabled, RADIUS servers can assign a VLAN ID to a port based on 802.1 authentication. If a user is authenticated, the user is assigned to this VLAN. When this feature is enabled on a port, each user is individually authenticated.

- **Guest VLAN**. From the menu, select **Enable** to enable the guest VLAN on the port. By default, the guest VLAN is disabled on all ports. For more information about the guest VLAN, see *Configure Global 802.1X Settings* on page 241.
- **Periodic Reauthentication**. From the menu, select **Enable** to allow periodic reauthentication of the supplicant for the port. By default, periodic reauthentication is disabled and connected clients are not forced to reauthenticate periodically.
- **Reauthentication Period**. Specify the time, in seconds, after which reauthentication of the supplicant occurs. The reauthentication period must be a value in the range of 300–4294967295 seconds. The default value is 3600 seconds.
- **Quiet Period**. Specify the number of seconds that the port remains in the quiet state following a failed authentication exchange. The valid range is 30–65535, and the default value is 60 seconds. 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 value, in seconds, after which an EAPoL EAP Request/Identify frame is resent to the supplicant. The valid range is 30–65535 seconds, and the default value is 30 seconds.
- **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. The valid range is 1–10, and the default value is 2.
- **Supplicant Timeout**. Specify the supplicant time-out for the selected port. The supplicant time-out is the value, in seconds, after which the supplicant times out. The valid range is 1–65535 seconds, and the default is 30 seconds.
- **Server Timeout**. Specify the time that elapses before the switch resends a request to the authentication server. The valid range is 1–65535 seconds, and the default is 30 seconds.

9. Click the **Apply** button.

   Your settings are saved.

The following table describes the nonconfigurable port authentication status information available on the page.

Table 57. Port authentication status information

Field	Description
Control Direction	The control direction for the specified port, which is always Both. The control direction dictates the degree to which protocol exchanges take place between supplicant and authenticator.The unauthorized controlled port exerts control over communication in both directions (disabling both incoming and outgoing frames).
Protocol Version	The protocol version associated with the selected port. The only possible value is 1, corresponding to the first version of the 802.1X specification.
PAE Capabilities	The port access entity (PAE) functionality of the selected port. Possible values are Authenticator or Supplicant.
Authenticator PAE State	The current state of the authenticator PAE state machine. Possible values are as follows: • Initialize • Disconnected • Connecting • Authenticating • Authenticated • Aborting • Held • ForceAuthorized • ForceUnauthorized
Backend State	The current state of the backend authentication state machine. Possible values are as follows: • Request • Response • Success • Fail • Timeout • Initialize • Idle

View the Port Summary

Use the Port Summary page to 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Port Authentication > Advanced > Port Summary**.

   The Port Summary page displays.

The following table describes the fields on the Port Summary page.

Table 58. 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. Possible values are as follows: • **Auto**. The authenticator port access entity (PAE) sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server. • **Force Authorized**. The authenticator PAE unconditionally sets the controlled port to authorized. The port can send and receive normal traffic without client port-based authentication. • **Force Unauthorized**. The authenticator PAE unconditionally sets the controlled port to unauthorized. The switch cannot provide authentication services to the client through the port.
Operating Control Mode	The control mode under which the port is actually operating. Possible values are as follows: • ForceUnauthorized • ForceAuthorized • Auto • N/A: If the port is in detached state, it cannot participate in port access control.
Reauthentication Enabled	This field shows whether reauthentication of the supplicant for the specified port is allowed. The possible values are TRUE and FALSE. If the value is TRUE, reauthentication occurs. Otherwise, reauthentication is not allowed.
Port Status	The authorization status of the specified port. The possible values are Authorized, Unauthorized, and N/A. If the port is in detached state, the value is N/A because the port cannot participate in port access control.

View the Client Summary

This page displays 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Port Authentication > Advanced > Client Summary**.

   The Client Summary page displays.

The following table describes the fields on the Client Summary page.

Table 59. Client Summary information

Field	Description
Port	The port for which information is displayed.
User Name	The user name that represents the identity of the supplicant device.
Supplicant Mac Address	The MAC address of the supplicant device.
Session Time	The time in seconds since the supplicant logged in.
VLAN ID	The VLAN ID assigned by the authenticator to the supplicant device.

Set Up Traffic Control

You can configure storm control, port security, protected port, and private VLAN settings.

From the **Security > Management Security > Traffic Control** menu, you can access the pages that are described in the following sections:

- *Configure Storm Control* on page 248
- *Configure Port Security* on page 249
- *Configure Protected Ports* on page 252
- *Configure Private VLANs* on page 252

Configure Storm Control

A broadcast storm is the result of an excessive number of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses can overload network resources, cause the network to time out, or do both.

The switch measures the incoming packet rate per port for broadcast, multicast, unknown, and unicast packets and discards packets if the rate exceeds the defined value. You enable storm control per interface, by defining the packet type and the rate at which the packets are transmitted.

Storm control is configured as a percentage of the maximum port speed.

➢ **To configure storm control settings:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Traffic Control > Storm Control**.

   The Storm Control page displays.

6. Select one or more ports by taking one of the following actions:
   - To configure a single port, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.

- To configure multiple ports with the same settings, select the check box associated with each port.
- To configure all ports with the same settings, select the check box in the heading row.

7. From the **Status** menus in the Unknown Unicast, Multicast, and Broadcast columns, select whether storm control is enabled or disabled. By default, storm control is disabled.

   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 the port, the traffic is dropped.

8. If the selection from a **Status** menu for a port is **Enable**, in the associated **Threshold** field, specify the maximum rate at which unknown unicast, multicast, or broadcast packets are forwarded.

   The range is a percent of the total threshold between 0 and 100%. The default is 5%. Storm control is configured as a percentage of the maximum port speed.

9. Click the **Apply** button.

   Your settings are saved.

Configure Port Security

Port security lets you lock one or more ports on the switch. When a port is locked, only packets with an allowable source MAC addresses can be forwarded. All other packets are discarded.

Configure a Port Security Interface

A MAC address can be defined as allowable by one of two methods: dynamically or statically. Both methods are used concurrently when a port is locked.

Dynamic locking implements a first arrival mechanism for port security. You specify how many addresses can be learned on the locked port. If the limit was not reached, then a packet with an unknown source MAC address is learned and forwarded normally. When the limit is reached, no more addresses are learned on the port. Any packets with source MAC addresses that were not already learned are discarded. You can effectively disable dynamic locking by setting the number of allowable dynamic entries to zero.

➢ **To configure port security settings:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Traffic Control > Port Security > Interface Configuration**.

   The Interface Configuration page displays.

6. Select which type of ports display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
7. Select one or more ports by taking one of the following actions:
   - To configure a single port, select the check box associated with the port, or type the port number in the **Go To Interface** field and click the **Go** button.
   - To configure multiple ports with the same settings, select the check box associated with each port.
   - To configure all ports with the same settings, select the check box in the heading row.
8. Specify the following port security settings:
   - **Port Security**. Enable or disable the port security feature for the selected ports. The default is Disable.
   - **Max Allowed Dynamically Learned MAC**. Specify the maximum number of dynamically learned MAC addresses on the selected ports. The valid range is 0–128. The default value is 128.
   - **Enable Violation Traps**. Enable or disable the sending of new violation traps if a packet with a disallowed MAC address is received. The default value is No, which means that the option is disabled.
9. Click the **Apply** button.

   Your settings are saved.

View Learned MAC Addresses and Convert Them to Static MAC Addresses

Use the Security MAC Address page to 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 *Access the Switch* on page 12.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Traffic Control > Port Security > Port Security Configuration**.

   The Port Security Configuration page displays.

6. Make sure that port security is globally enabled.

   For more information, see *Configure 802.1X Settings for a Port* on page 243.

7. Select **Security > Traffic Control > Port Security > Interface Configuration**.

   The Interface Configuration page displays.

8. Make sure that port security is enabled for the individual interface for which you want to view the dynamically learned MAC addresses.

   For more information, see *Configure a Port Security Interface* on page 249.

9. Select **Security > Traffic Control > Port Security > Security MAC Address**.

   The Port Settings page displays. The page also displays the Dynamic MAC Address Table section.

10. From the **Port List** menu, select an interface.

    The Number of Dynamic MAC Addresses Learned field displays the number of dynamically learned MAC addresses for the interface.

    The Dynamic MAC Address Table displays the MAC addresses and their associated VLANs that were learned on the selected interface.

Field	Description
VLAN ID	The VLAN ID corresponding to the MAC address.
MAC Address	The MAC addresses learned on the interface.

11. To convert the dynamically learned MAC addresses to a statically locked addresses, select the **Convert Dynamic Address to Static** check box.
12. Click the **Apply** button.

    The dynamic MAC addresses are converted to static MAC addresses in a numerically ascending order until the static limit is reached.

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

Configure Protected Ports

If a port is configured as protected, it does not forward traffic to any other protected port on the switch, but it does forward traffic to unprotected ports. Use the Protected Ports Membership page to configure the ports as protected or unprotected. You need read/write access privileges to modify the configuration.

➢ **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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Traffic Control > Protected Port**.

   The Protected Port Membership page displays.

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 Private VLANs

A private VLAN contains switch ports that cannot communicate with each other, but can access another network. These ports are called private ports. Each private VLAN contains one or more private ports and a single uplink port or uplink aggregation group. Note that all traffic between private ports is blocked at all layers, not just Layer 2 traffic, but also traffic such as FTP, HTTP, and Telnet.

From the **Security > Management Security > Traffic Control > Private Vlan** menu, you can access the pages that are described in the following sections:

- *Configure the Private VLAN Type* on page 253
- *Configure Private VLAN Association Settings* on page 254
- *Configure the Private VLAN Port Mode* on page 255

- *Configure a Private VLAN Host Interface* on page 256
- *Configure a Private VLAN Promiscuous Interface* on page 257

Configure the Private VLAN Type

➢ **To configure a private VLAN type:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Traffic Control > Private Vlan > Private Vlan Type Configuration**.

   The Private Vlan Type Configuration page displays.

6. Select the check box for the VLAN ID that you want to configure.
7. From the **Private VLAN Type** menu, select the type of private VLAN. Possible values are as follows:
   - **Unconfigured**. Sets the private VLAN type as unconfigured. This is the default selection.
   - **Primary**. Sets the private VLAN type as primary, which allows Layer 2 connectivity from promiscuous ports to isolated ports and to community ports.
   - **Isolated**. Sets the private VLAN type as isolated, which allows isolated ports to send traffic to the primary VLAN and to promiscuous ports.
   - **Community**. Sets the private VLAN type as community, which allows Layer 2 connectivity from community ports to promiscuous ports and to community ports of the same community.
8. Click the **Apply** button.

   Your settings are saved.

Configure Private VLAN Association Settings

➢ **To configure private VLAN association:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Traffic Control > Private Vlan > Private Vlan Association Configuration**.

   The Private Vlan Association Configuration page displays.

6. From the **Primary VLAN** menu, select the primary VLAN ID of the domain.

   You can select only a VLAN that you previously configured as a primary VLAN (see *Configure the Private VLAN Type* on page 253).

7. In the **Secondary VLAN(s)** field, enter the VLAN that you want to associate with the primary VLAN.

   You can specify statically created VLANs (excluding the primary and default VLANs).

   You can associate a single, isolated VLAN and multiple community VLANs with the selected primary VLAN.

8. Click the **Apply** button.

   Your settings are saved.

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

Table 60. Private Vlan Association Configuration information

Field	Description
Isolated VLAN	The isolated VLAN that is associated with the selected primary VLAN.
Community VLAN(s)	The list of community VLANs that are associated with the selected primary VLAN.

Configure the Private VLAN Port Mode

➢ **To configure the private VLAN port 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Traffic Control > Private Vlan > Private Vlan Port Mode Configuration**.

   The Private Vlan Port Mode Configuration page displays.

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. From the **Port VLAN Mode** menu, select the switch port mode:
   - **General**. Sets the interface in general mode, which is the default selection. General mode means that the interface is not a private VLAN port.
   - **Private VLAN Promiscuous**. Sets the interface in promiscuous mode, which is used for private VLAN promiscuous interface configurations. For more information, see *Configure a Private VLAN Promiscuous Interface* on page 257.
   - **Private VLAN Host**. Sets the interface in host mode, which is used for private VLAN host interface configurations. For more information, see *Configure a Private VLAN Host Interface* on page 256.

8. Click the **Apply** button.

   Your settings are saved.

Configure a Private VLAN Host Interface

➢ **To configure a private VLAN host 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Traffic Control > Private Vlan > Private Vlan Host Interface Configuration**.

   The Private Vlan Host Interface Configuration page displays.

6. Select which type of interfaces display onscreen:
   - To display physical interfaces only, click **PORTS**.
   - To display LAGs only, click **LAGS**.
   - To display both physical interfaces and LAGs, click **All**.
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 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.
8. In the **Host Primary VLAN** field, enter the primary VLAN ID for the host association mode.

   The range of the VLAN ID is 2–4093. You can enter only a VLAN that you previously configured as a primary VLAN (see *Configure the Private VLAN Type* on page 253).

9. In the **Host Secondary VLAN** field, enter the secondary VLAN ID for host association mode.

   The range of the VLAN ID is 2–4093. You can enter only a VLAN that you previously configured as a secondary VLAN (see *Configure Private VLAN Association Settings* on page 254).

10. Click the **Apply** button.

    Your settings are saved.

    The Operational VLAN(s) field displays the operational VLANs.

Configure a Private VLAN Promiscuous Interface

➢ **To configure a private VLAN promiscuous 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > Traffic Control > Private Vlan > Private Vlan Promiscuous Interface Configuration**.

   The Private Vlan Promiscuous Interface Configuration page displays.

6. Select which type of interfaces display onscreen:
   - To display physical interfaces only, click **PORTS**.
   - To display LAGs only, click **LAGS**.
   - To display both physical interfaces and LAGs, click **All**.
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 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.
8. In the **Promiscuous Primary VLAN** field, enter the primary VLAN ID for the promiscuous association mode.

   The range of the VLAN ID is 2–4093. You can enter only a VLAN that you previously configured as a primary VLAN (see *Configure the Private VLAN Type* on page 253).

9. In the **Promiscuous Secondary VLAN** field, enter the secondary VLAN ID for promiscuous association mode.

This field can accept single a VLAN ID, a range of VLAN IDs, or a combination of both in sequence separated by a comma. You can specify an individual VLAN ID, such as 10. You can specify the VLAN range values separated by a hyphen, for example, 10-13. You can specify the combination of both separated by commas, for example, 12,15,40-43,1000-1005, 2000. The range of VLAN IDs is 2–4093.

Note: The VLAN ID list that you specify replaces the configured secondary VLAN list in the association.

10. Click the **Apply** button.

    Your settings are saved.

    The Operational VLAN(s) field displays the operational VLANs.

Configure Access Control Lists

Access control lists (ACLs) ensure that only authorized users can access specific resources while blocking off any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and above all provide security for the network. The switch supports IPv4, IPv6, and MAC ACLs.

➢ **To configure an ACL:**

1. Create an IPv4-based, IPv6-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 333.

From the **Security > Management Security > ACL** menu, you can access the pages that are described in the following sections:

- *Use the ACL Wizard to Create a Simple ACL* on page 259
- *Configure a Basic MAC ACL* on page 264
- *Configure MAC ACL Rules* on page 266
- *Configure MAC Bindings* on page 270
- *View or Delete MAC ACL Bindings in the MAC Binding Table* on page 271
- *Configure an IP ACL* on page 272
- *Configure Rules for a Basic IP ACL* on page 274
- *Configure Rules for an Extended IP ACL* on page 277
- *Configure an IPv6 ACL* on page 281
- *Configure IPv6 Rules* on page 283

- *Configure IP ACL Interface Bindings* on page 286
- *View or Delete IP ACL Bindings in the IP ACL Binding Table* on page 288

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 an IP ACL* on page 272.

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 (for 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 *Access the Switch* on page 12.

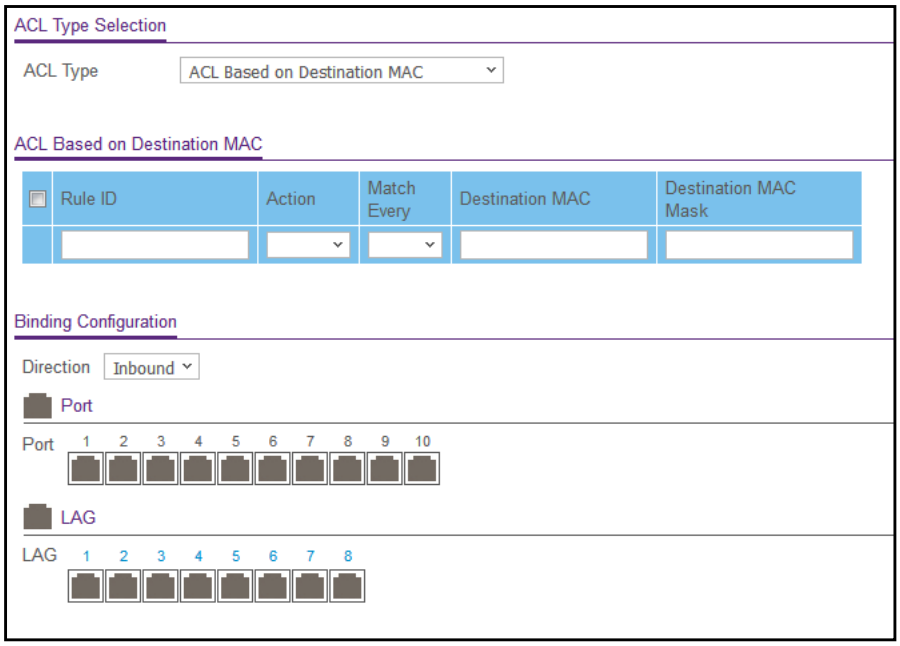
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > ACL Wizard**.



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 IPv6**. Creates an ACL based on the destination IPv6 prefix and IPv6 prefix length.
   - **ACL Based on Source IPv6.** Creates an ACL based on the source IPv6 prefix and IPv6 prefix length.
   - **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.
   - **ACL Based on Destination IPv6 L4 Port**. Creates an ACL based on the destination IPv6 Layer 4 port number.
   - **ACL Based on Source IPv6 L4 Port**. Creates an ACL based on the source IPv6 Layer 4 port number.

   Note: For L4 port options, two rules are created (one for TCP and one for UDP).

7. In the **Rule ID** field, enter a whole number in the range of 1 to 50 that is used to identify the rule.
8. From the **Action** menu, select **Permit** or **Deny** to specify the action that must be taken if a packet matches the rule's criteria.
9. From the **Match Every** menu, select one of the following options:
   - **False**. Signifies that packets do not need to match the selected ACL and rule. With this selection, you can add a destination MAC address, destination MAC mask, and VLAN.
   - **True**. Signifies that all packets must match the selected ACL and rule and are either permitted or denied. In this case, since all packets match the rule, the option of configuring other match criteria is not offered.
10. Specify the additional match criteria for the selected ACL type.

    The 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 valid format is xx:xx:xx:xx:xx:xx. The BPDU keyword might be specified using a destination MAC address of 01:80:C2:xx:xx:xx. • **Destination MAC Mask**. Specify the destination MAC address mask, which represents the bits in the destination MAC address to compare against an Ethernet frame. The valid format is xx:xx:xx:xx:xx:xx. The BPDU keyword might be specified using a destination MAC mask of 00:00:00:ff:ff:ff.
Source MAC	• **Source MAC**. Specify the source MAC address to compare against an Ethernet frame. The valid format is xx:xx:xx:xx:xx:xx. • **Source MAC Mask**. Specify the source MAC address mask, which represents the bits in the source MAC address to compare against an Ethernet frame. The valid format is (xx:xx:xx:xx:xx:xx).
Destination IPv4	• **Destination IP Address**. Specify the destination IP address. • **Destination IP Mask**. Specify the destination IP address mask.
Source IPv4	• **Source IP Address**. Specify the source IP address. • **Source IP Mask**. Specify the source IP address mask.
Destination IPv6	• **Destination Prefix**. Specify the destination prefix. • **Destination Prefix Length**. Specify the destination prefix length.
Source IPv6	• **Source Prefix**. Specify the source destination prefix. • **Source Prefix Length**. Specify the source prefix length.
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.

ACL Based On	Fields
Destination IPv6 L4 Port	• **Destination L4 port (protocol)**. Specify the destination IPv6 L4 port protocol. • **Destination L4 port (value)**. Specify the destination IPv6 L4 port value.
Source IPv6 L4 Port	• **Source L4 port (protocol)**. Specify the source IPv6 L4 port protocol. • **Source L4 port (value)**. Specify the source IPv6 L4 port value.

11. In the Binding Configuration section, from the **Direction** menu, select the packet filtering direction for the ACL.

    Only the inbound direction is valid.

12. In the Ports and LAG tables in the Binding Configuration section, click each port and LAG to which the ACL must be applied.

    Selected ports and LAGs are marked with a check mark.

13. Click the **Add** button.

    The rule is added to the ACL.

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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > ACL Wizard**.

   The ACL Wizard page displays.

6. Select check box for 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

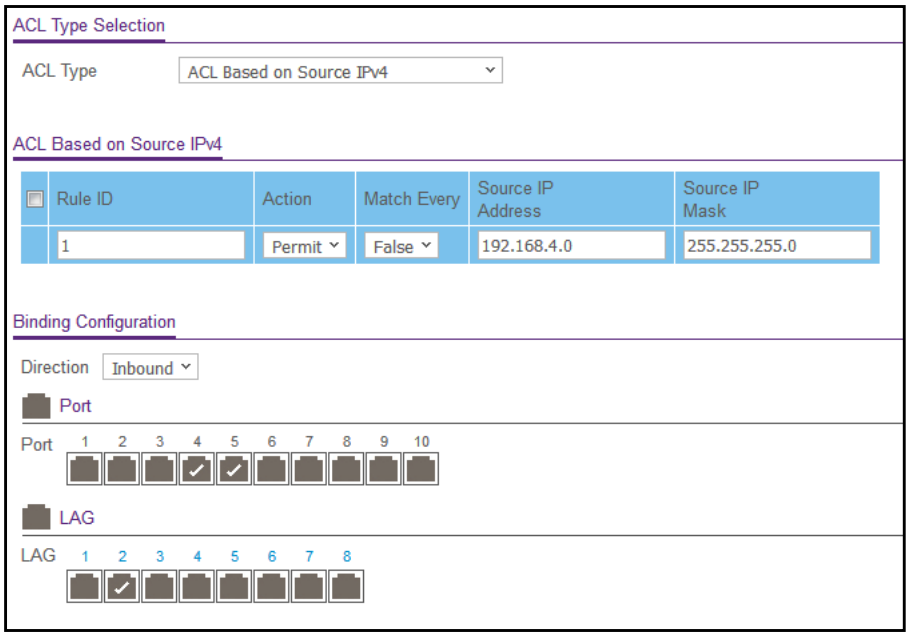
5. Select **Security > ACL > ACL Wizard**.

   The ACL Wizard page displays.

6. Select check box for the rule.
7. Click the **Delete** button and the rule is removed.

ACL Wizard Example

In the following figure, the ACL rule is configured to check for packet matches on ports 4 and 5 and on LAG 2. 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.



For information about the ACL Wizard, see *Use the ACL Wizard to Create a Simple ACL* on page 259.

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 the ACL ID.
2. Create a MAC rule.
3. Associate the MAC ACL with one or more interfaces.

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 271.

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 *Access the Switch* on page 12.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Basic > MAC ACL**.

   The MAC ACL Table page displays.

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 only.

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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Basic > MAC ACL**.

   The MAC ACL page displays.

6. Select check box for the rule.
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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Security > ACL > Basic > MAC ACL**.

   The MAC ACL page displays.
6. Select check box for the rule.
7. Click the **Delete** button.

   The rule is removed.

Configure MAC ACL Rules

Use the MAC Rules page to define rules for MAC-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. A default *deny all* rule is the last rule of every list.

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.

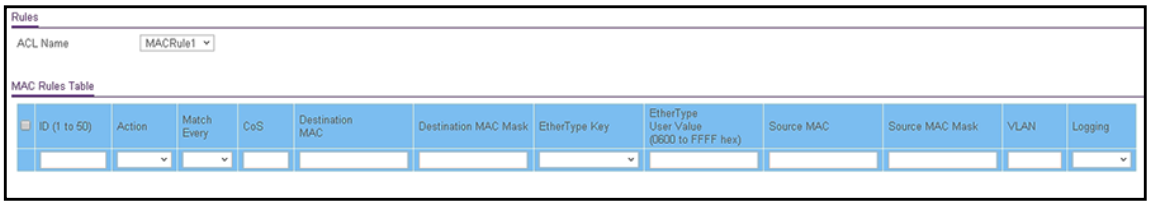
   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

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

   The default password is **password**.

The System Information page displays.

5. Select **Security > ACL > Basic > MAC Rules**.



The previous figure does not show all columns.

6. From the **ACL Name** menu, select the MAC ACL.

   For information about adding MAC ACLs, see *Configure a Basic MAC ACL* on page 264.

7. In the **ID** field, enter a whole number in the range of 1 to 50 to identify the rule.
8. 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.
9. In the **CoS** field, specify the 802.1p user priority that must be compared against the information in an Ethernet frame.

   The range of valid values is 0 to 7.

10. In the **Destination MAC** field, specify the destination MAC address that must be compared against the information in an Ethernet frame.

    The valid format is xx:xx:xx:xx:xx:xx.

11. In the **Destination MAC Mask** field, specify the destination MAC address mask that must be compared against the information in an Ethernet frame.

    The MAC address mask specifies which bits in the destination MAC to compare against an Ethernet frame. Use Fs and 0s in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a 0 in a bit position means that the data must equal the value given for that bit. For example, if the MAC address is aa:bb:cc:dd:ee:ff, and the mask is 00:00:ff:ff:ff:ff, all MAC addresses with aa:bb:xx:xx:xx:xx result in a match (where x is any hexadecimal number). A MAC mask of 00:00:00:00:00:00 matches a single MAC address.

12. From the **EtherType Key** menu, select the EtherType value that must be compared against the information in an Ethernet frame.

    The valid values are as follows:

    - **Appletalk**
    - **ARP**
    - **IBM SNA**
    - **IPv4**
    - **IPv6**

- **IPX**
- **MPLS multicast**
- **MPLS unicast**
- **Netbios**
- **Novell**
- **PPPoE**
- **Reverse ARP**
- **User Value**

13. If you select **User Value** from the **EtherType Key** menu, specify a customized EtherType value in the **EtherType User Value** field.

    This value must be compared against the information in an Ethernet frame. The range of valid values is 0x0600 to 0xFFFF.

14. In the **Source MAC** field, specify the source MAC address that must be compared against the information in an Ethernet frame.

    The valid format is xx:xx:xx:xx:xx:xx.

15. In the **Source MAC Mask** field, specify the source MAC address mask that must be compared against the information in an Ethernet frame.

    Use Fs and 0s in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a 0 in a bit position means that the data must equal the value given for that bit. The valid format is xx:xx:xx:xx:xx:xx. A MAC mask of 00:00:00:00:00:00 matches a single MAC address.

16. In the **VLAN** field, specify the VLAN ID that must be compared against the information in an Ethernet frame.

    The range of valid values is 1 to 4093.

17. From the **Logging** menu, select whether to enable or disable logging.

    When set to **Enable**, logging is enabled for this ACL rule (subject to resource availability on the switch). If the access list trap flag is also enabled, periodic traps are generated, indicating the number of times the rule was evoked during the report interval. A trap is not issued if the ACL rule hit count is zero for the interval. This field is supported only for a deny action.

18. 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Basic > MAC Rules**.

   The MAC Rules page displays.

6. Select the check box for 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Basic > MAC Rules**.

   The MAC Rules page displays.

6. Select the check box for 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. Use the MAC Binding Configuration page to assign MAC ACL lists to ACL priorities and interfaces.

➢ **To configure MAC bindings:**

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

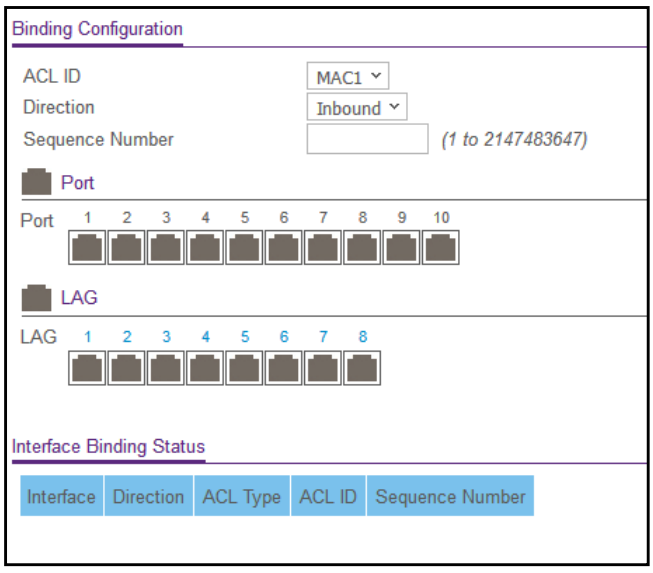
   You can use a WiFi or wired connection to connect your computer to the network, or connect directly to a switch that is off-network using an Ethernet cable.
2. Launch a web browser.
3. In the address field of your web browser, enter the IP address of the switch.

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Security > ACL > Basic > MAC Binding Configuration**.



6. From the **ACL ID** menu, select a MAC 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 this interface and direction is used. The valid range is 1–2147483647.

8. To add the selected ACL to a port or LAG, in the Ports table or LAG table, click the port or LAG so that a check mark displays.

   You can add the ACL to several ports and LAGs.

   The Ports and LAG tables display the available and valid interfaces for ACL binding. All nonrouting physical interfaces and interfaces participating in LAGs are listed.

9. Click the **Apply** button.

   Your settings are saved.

The following table describes the information displayed in the Interface Binding Status table.

Table 61. Interface Binding Status table

Field	Description
Interface	The interface of the ACL assigned.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID	The ACL number (for an IP ACL) or ACL name for a MAC ACL) identifying the ACL assigned to the selected interface and direction.
Sequence Number	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.

View or Delete MAC ACL Bindings in the MAC Binding Table

You can view or delete the MAC ACL bindings in the MAC Binding Table.

➢ **To view or delete MAC ACL bindings:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security** > **ACL > Basic** > **MAC Binding Table**.

   The MAC Binding Table page displays.

6. To delete a MAC ACL-to-interface binding, do the following:
   a. Select the check box for 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 62. MAC Binding Table

Field	Description
Interface	The interface of the ACL assigned.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID	The ACL name identifying the ACL assigned to the selected interface and direction.
Sequence Number	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.

Configure an IP ACL

An IP or IPv6 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.

Use the IP ACL page to add or remove IP-based ACLs.

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 *Access the Switch* on page 12.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Advanced > IP ACL**.

   The IP ACL Table page displays.

6. In the **IP ACL ID** field, specify the ACL ID, 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.

   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 an ID from 1 to 99) or extended IP ACL (with an ID from 100 to 199).

7. Click the **Add** button.

   The IP ACL is added to the switch configuration.

Delete an IP ACL

➢ **To delete an IP ACL:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Advanced > IP ACL**.

The IP ACL Configuration page displays.

6. Select the check box for the IP ACL.
7. Click the **Delete** button.

   The IP ACL is removed.

Configure Rules for a Basic IP ACL

Use the IP Rules page to 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 *Access the Switch* on page 12.

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

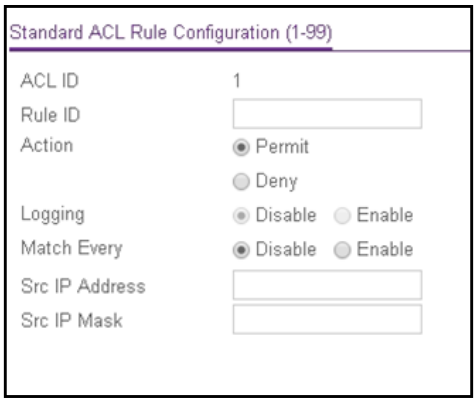
   The default password is **password**.

   The System Information page displays.
5. Select **Security > ACL > Advanced > IP Rules**.

   The IP Rules table displays. The page also shows the Basic ACL Rule Table section.

   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:
   - **Rule ID**. Enter an ACL sequence number in the range of 1 to 50 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.
     - **Deny**. Drop packets that meet the ACL criteria.
   - **Logging**. If the selection from the **Action** menu is **Deny**, you can enable logging for the ACL by selecting the **Enable** radio button. (Logging is subject to resource availability in the device.)

     If the access list trap flag is also enabled, periodic traps are generated, indicating the number of times this rule was evoked during the report interval. A fixed five-minute report interval is used for the switch. A trap is not issued if the ACL rule hit count is zero for the current interval.
   - **Match Every**. Select a radio button 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.
   - **Src IP Address**. Enter an IP address using dotted-decimal notation to be compared to a packet's source IP address as a match criterion for the selected IP ACL rule.
   - **Src IP Mask**. Specify the IP mask in dotted-decimal notation to be used with the source IP address value.
9. Click the **Apply** button.

   The new rule is added to the Basic ACL Rule Table on the IP Rules page and the fields on the Standard ACL Rule Configuration (1-99) page are automatically cleared so that you can add another rule (if you want to).

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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Security > ACL > Advanced > IP 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 (1-99) 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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Advanced > IP 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 for the rule.
8. Click the **Delete** button.

   The rule is removed.

Configure Rules for an Extended IP ACL

Use the IP Extended Rules page to define rules for IP-based extended ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded.

Note: 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 *Access the Switch* on page 12.

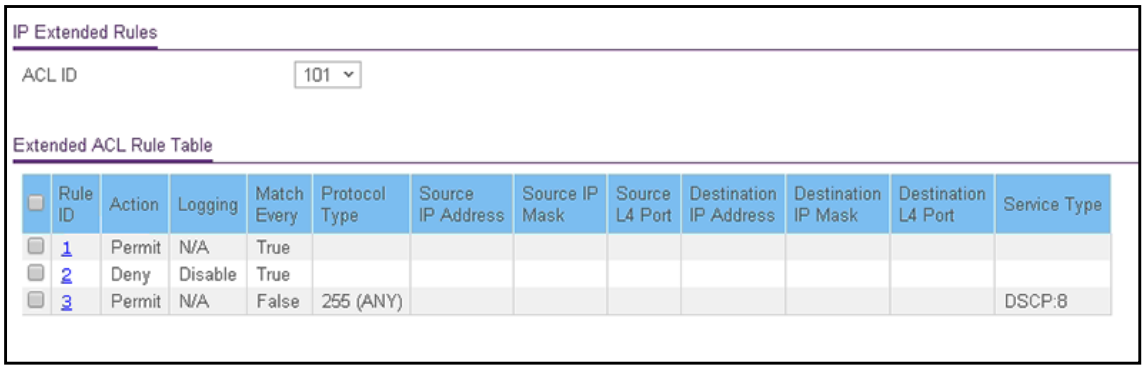
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Advanced > IP Extended Rules**.

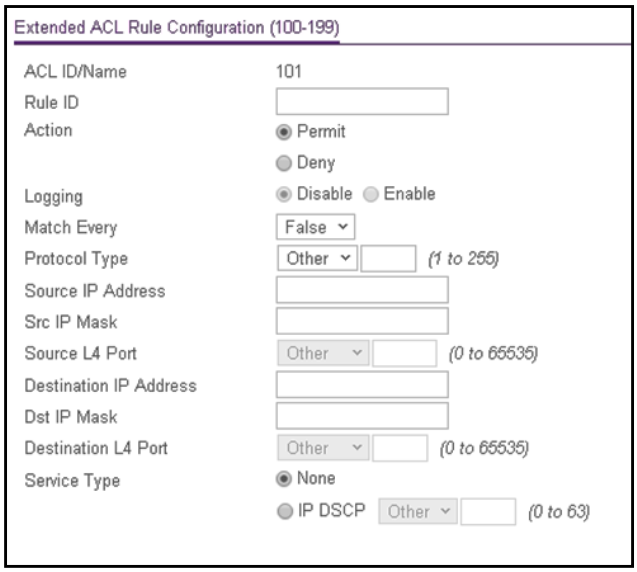


If one or more rules exist for the ACL, the rules display in the Extended ACL Rule Table.

6. From the **ACL ID/Name** menu, select the IP ACL for which you want to add a rule.

   For extended IP ACLs, this must be an ID in the range from 101 to 199.

7. Click the **Add** button.



8. Configure the following match criteria for the rule:
   - **Rule ID**. Enter a whole number in the range of 1 to 50 that is used to identify the rule. An extended IP ACL can contain up to 50 rules.
   - **Action**. Select the ACL forwarding action, which is one of the following:
     - **Permit**. Forward packets that meet the ACL criteria.
     - **Deny**. Drop packets that meet the ACL criteria.
   - **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.)

     If the access list trap flag is also enabled, periodic traps are generated, indicating the number of times this rule was evoked during the report interval. A fixed five-minute

report interval is used for the switch. A trap is not issued if the ACL rule hit count is zero for the current interval.

- **Match Every**. From the **Match Every** menu, select whether all packets must match the selected IP ACL rule:
  - **False**. Not all packets need to match the selected IP ACL rule. You can configure other match criteria on the page.
  - **True**. All packets must match the selected IP ACL rule and are either permitted or denied. In this case, you cannot configure other match criteria on the page.
- **Protocol Type**. From the menu, select a protocol that a packet's IP protocol must be matched against: **IP**, **ICMP**, **IGMP**, **TCP**, **UDP**, or **Other**. If you select **Other**, enter a protocol number from 0 to 255.
- **Source IP Address**. In the **Source IP Address** 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.
- **Src IP Mask**. In the **Src IP Mask** field, enter a source IP mask, using dotted-decimal notation, to be compared to a packet's source IP mask as a match criterion for the selected IP ACL rule.

  Wildcard masks determine which bits are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that *none* of the bits are important. A wildcard mask of 0.0.0.0 indicates that *all* of the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. For example, to apply the rule to all hosts in the 192.168.1.0/24 subnet, enter 0.0.0.255 in the **Src IP Mask** field. This field is required when you configure a source IP address.
- **Source L4 port**. 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.

  The source port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **http**, **smtp**, **snmp**, **telnet**, **tftp**, and **www**. Each of these values translates into its equivalent port number.

  Select **Other** from the menu to enter a port number from 0 to 65535.
- **Destination IP Address**. In the **Destination IP Address** 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.
- **Dst IP Mask**. In the **Dst IP Mask** field, enter a destination IP mask, using dotted-decimal notation, to be compared to a packet's destination IP mask as a match criterion for the selected IP ACL rule.

  Wildcard masks determine which bits are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that *none* of the bits are important. A wildcard mask of 0.0.0.0 indicates that *all* of the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. For example, to apply the rule to all hosts in the 192.168.1.0/24 subnet, enter 0.0.0.255 in the **Dst IP Mask** field. This field is required when you configure a destination IP address.

- **Destination L4 port**. 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.

  The destination port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **http**, **smtp**, **snmp**, **telnet**, **tftp**, and **www**. Each of these values translates into its equivalent port number.

  Select **Other** from the menu to enter a port number from 0 to 65535.

- **Service Type**. Select either the **None** radio button to ignore a service type match condition or the **IP DSCP** radio button for an IP DSCP service type match condition for the extended IP ACL rule.

  If you select the **IP DSCP** radio button, select one of the IP DiffServ Code Point (DSCP) keywords from the menu. The DSCP is defined as the high-order 6 bits of the service type octet in the IP header. To specify a numeric value, select **Other** from the menu and enter a numeric value from 0 to 63.

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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Advanced > IP Extended Rules**.

   The IP Extended 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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Security > ACL > Advanced > IP Extended Rules**.

   The Extended 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 for the rule.
8. Click the **Delete** button.

   The rule is removed.

Configure an IPv6 ACL

An IP or IPv6 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. On this page the interfaces to which an IP ACL applies must be specified, as well as whether it applies to inbound or outbound traffic. You can create rules for the IPv6 ACL on the IPv6 Rules page.

Add an IPv6 ACL

➢ **To add an IPv6 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Advanced > IPv6 ACL**.

   The IPv6 ACL Table page displays.

6. In the **IPv6 ACL** field, specify a name, number, or combination of both to identify the IPv6 ACL.

   The IPv6 ACL string can include up to 31 alphanumeric characters only. The name must start with an alphabetic character.

7. Click the **Add** button.

   The IPv6 ACL is added.

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

Table 63. IPv6 ACL Table information

Field	Description
Rules	The number of the rules that are associated with the IP ACL.
Type	The type is IPv6 ACL.

Delete an IPv6 ACL

➢ **To delete an IPv6 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Advanced > IPv6 ACL**.

   The IPv6 ACL Table page displays.

6. Select the check box for the IPv6 ACL.
7. Click the **Delete** button.

The IPv6 ACL is removed.

Configure IPv6 Rules

Use these pages to display the rules for the IPv6 access control lists, which are created using the IPv6 Access Control List Configuration page. By default, no specific value is in effect for any of the IPv6 ACL rules.

Add a Rule for an IPv6 ACL

➢ **Add a rule for an ACL IPv6:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

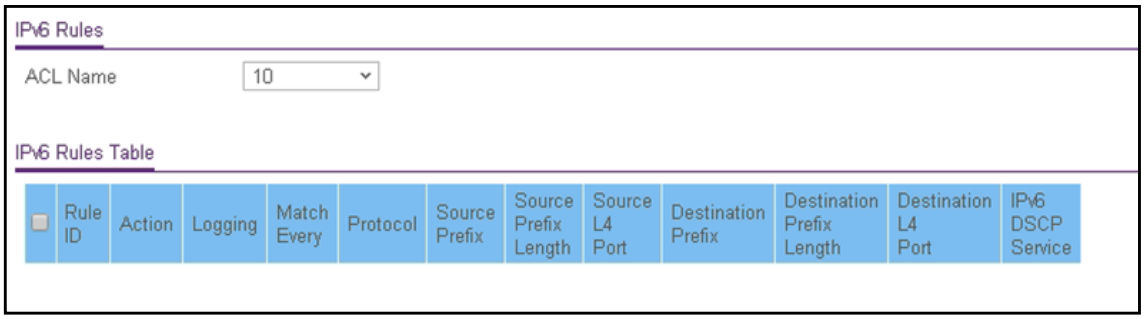
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

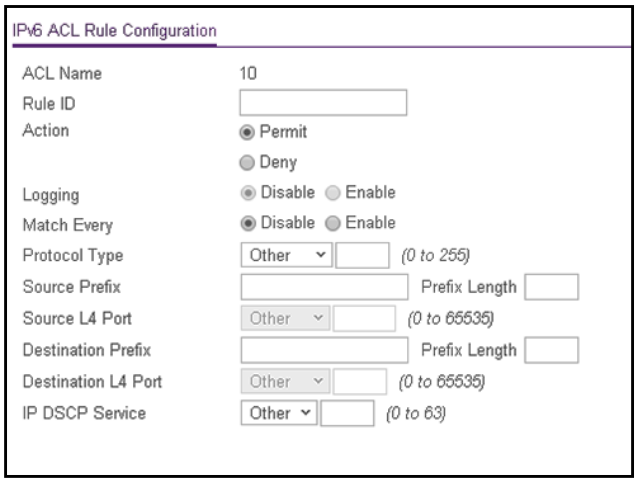
5. Select **Security > ACL > Advanced > IPv6 Rules**.



6. From the **ACL Name** menu, select the IPv6 ACL for which you want to add a rule.

   An IPv6 ACL can contain up to 50 rules.

7. Click the **Add** button.



8. Configure the following match criteria for the rule:
   - **Action**. Select the ACL forwarding action by selecting one of the following radio buttons:
     - **Permit**. Forward packets that meet the ACL criteria.
     - **Deny**. Drop packets that meet the ACL criteria.
   - **Logging**. If you select the **Deny** radio button, you can enable logging for the ACL by selecting the **Enable** radio button. (Logging is subject to resource availability in the device.)

     If the access list trap flag is also enabled, periodic traps are generated, indicating the number of times this rule was evoked during the report interval. A fixed five-minute report interval is used for the switch. A trap is not issued if the ACL rule hit count is zero for the current interval.
   - **Match Every**. Select whether all packet must match the selected IPv6 ACL rule:
     - **Disable**. Not all packets need to match the selected IPv6 ACL rule. You can configure other match criteria on the page.
     - **Enable**. All packets must match the selected IPv6 ACL rule and are either permitted or denied. In this case, you cannot configure other match criteria on the page.
   - **Protocol Type**. Specify the IPv6 protocol type in one of the following ways:
     - From the **Protocol Type** menu, select **IPv6**, **ICMPv6**, **TCP**, or **UDP**.
     - From the **Protocol Type** menu, select **Other**, and in the associated field, specify an integer ranging from 0 to 255. This number represents the IPv6 protocol.
   - **Source Prefix** and **Prefix Length**. In the **Source Prefix** field and **Prefix Length** field, enter the IPv6 prefix combined with the IPv6 prefix length of the network or host from which the packet is being sent. The valid range for the prefix length is 0–128.
   - **Source L4 port**. 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 IPv6 ACL rule.

The source port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **http**, **smtp**, **snmp**, **telnet**, **tftp**, and **www**. Each of these values translates into its equivalent port number.

Select **Other** from the menu to enter a port number from 0 to 65535.

- **Destination Prefix** and **Prefix Length**. In the **Destination Prefix** field and **Prefix Length** field, enter the IPv6 prefix combined with the IPv6 prefix length of the network or host to which the packet is being sent. The valid range for the prefix length is 0–128.
- **Destination L4 port**. 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 IPv6 ACL rule.

  The source port protocols are **domain**, **echo**, **ftp**, **ftpdata**, **http**, **smtp**, **snmp**, **telnet**, **tftp**, and **www**. Each of these values translates into its equivalent port number.

  Select **Other** from the menu to enter a port number from 0 to 65535.
- **IPv6 DSCP Service**. Specify the IP DiffServ Code Point (DSCP) field. This is an optional configuration.

  Select one of the IP DiffServ Code Point (DSCP) keywords from the menu. The DSCP is defined as the high-order 6 bits of the service type octet in the IP header. To specify a numeric value, select **Other** from the menu and enter a numeric value from 0 to 63.

9. Click the **Apply** button.

   Your settings are saved.

Modify the Match Criteria for an IPv6 ACL Rule

➢ **To modify the match criteria for an IPv6 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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Security > ACL > Advanced > IPv6 Rules**.

   The IPv6 Rules page displays.
6. From the **ACL Name** menu, select the ACL that includes the rule that you want to modify.

7. In the IPv6 ACL Rules Table, click the rule.

   The rule is a hyperlink. The IPv6 ACL Rule Configuration page displays.

8. Modify the IPv6 ACL rule criteria.
9. Click the **Apply** button.

   Your settings are saved.

Delete an IPv6 ACL Rule

➢ **To delete an IPv6 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Advanced > IPv6 Rules**.

   The IPv6 Rules page displays.

6. From the **ACL Name** menu, select the ACL that includes the rule that you want to delete.
7. In the IPv6 ACL Rules Table, select the check box for the rule.
8. Click the **Delete** button.

   The rule is removed.

Configure IP ACL Interface Bindings

When an ACL is bound to an interface, all the rules that are defined are applied to the selected interface. Use the IP Binding Configuration page to assign ACL lists to ACL priorities and interfaces.

If resources on the switch are insufficient, an attempt to bind an ACL to an interface fails. You cannot bind an IPv4 ACL and an IPv6 ACL to the same interface.

➢ **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 *Access the Switch* on page 12.

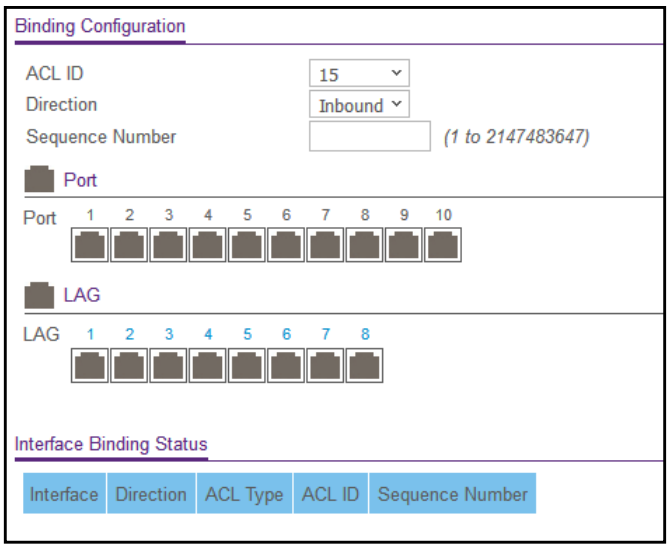
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Advanced > IP Binding Configuration**.



6. From the **ACL ID** menu, select an existing IP ACL for which you want to add an IP ACL interface binding.

   The fixed selection from the **Direction** menu is **Inbound**, which means that ACL rules are applied to traffic entering the interface.

7. In the **Sequence Number** field, optionally specify a number to indicate the order of the access list relative to other access lists already assigned to this interface and direction.

   A low number indicates high precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If you do not specify the sequence number (meaning that the value is 0), a sequence number that is one number greater than the highest sequence number currently in use for this interface and direction is used. The valid range is 1–2147483647.

8. To add the selected ACL to a port or LAG, in the Ports table or LAG table, click the port or LAG so that a check mark displays.

   You can add the ACL to several ports and LAGs.

   The Ports and LAG tables display the available and valid interfaces for ACL bindings. All nonrouting physical 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 64. Interface Binding Status table information

Field	Description
Interface	The selected interface.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID	The ACL number (for an IP ACL) or ACL name (for a named IPv6 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

Use the IP Binding Table page to view or delete the IP ACL bindings.

➢ **To view or delete IP ACL bindings:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Security > ACL > Advanced > Binding Table**.

   The IP Binding Table page displays.

6. To delete an IP ACL-to-interface binding, do the following:
   a. Select the check box for the interface.
   b. Click the **Delete** button.

      The binding is removed.

The following table describes the information displayed in the IP Binding Status table.

Table 65. IP Binding Status table information

Field	Description
Interface	The selected interface.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID	The ACL number (for an IP ACL) or ACL name (for a named IPv6 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.

Monitor the System

7

This chapter covers the following topics:

- *Monitor the Switch and the Ports*
- *Configure and View Logs*
- *Configure Port Mirroring*
- *View the System Resource Utilization*

Monitor the Switch and the Ports

The pages available from the **Monitoring > Ports** menu contain a variety of information about the number and type of traffic transmitted from and received on the switch.

From the **Monitoring > Ports** menu, you can access links to the features described following sections:

- *Switch Statistics* on page 291
- *View Port Statistics* on page 292
- *View Detailed Port Statistics* on page 295
- *View EAP Statistics* on page 298
- *Perform a Cable Test* on page 300

Switch Statistics

The Switch Statistics page displays detailed statistical information about the traffic the switch handles.

➢ **To view and clear the switch statistics:**

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

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

   If you do not know the IP address of the switch, see *Access the Switch* 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. To view the switch statistics, select **Monitoring > Ports > Switch Statistics**.

   The Statistics page displays.
6. Click the **Refresh** button to refresh the page with the latest information about the switch.
7. Click the **Clear** button to clear all the statistics counters, resetting all switch summary and detailed statistics to default values.

   The discarded packets count cannot be cleared.

The following table describes the switch statistics displayed on the page.

Table 66. Switch statistics information

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).
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. This does not include multicast packets.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
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.
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.
Static VLAN Entries	The number of active VLAN entries on this switch that were created statically.

View Port Statistics

The Port Statistics page displays 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 *Access the Switch* on page 12.

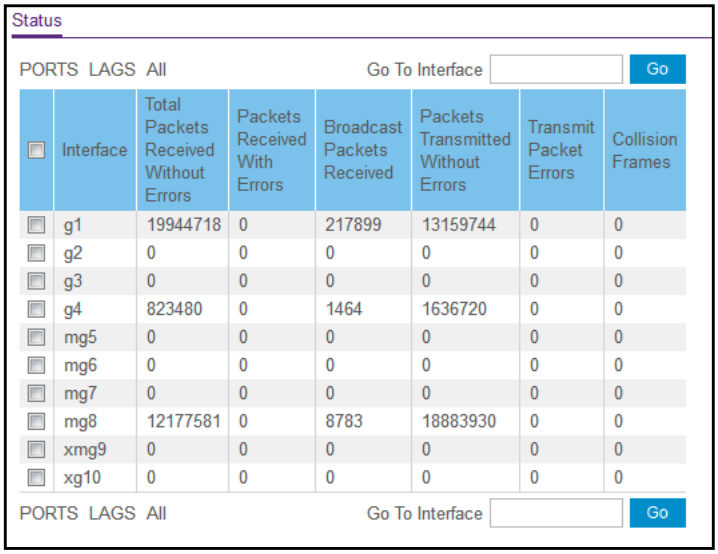
   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Ports > Port Statistics**.



6. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
7. To view information about a single interface, type the interface number in the **Go To Interface** field, and click the **Go** button.
8. Click the **Refresh** button to refresh the page with the latest information about the switch.

The following table describes the per-port statistics displayed on the page.

Table 67. Port Status information

Field	Description
Interface	This object indicates the interface of the interface table entry associated with this port on an adapter.
Total Packets Received Without Errors	The total number of packets received that were without errors.
Packets Received With Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. This does not include multicast packets.
Packets Transmitted Without Errors	The number of frames that were transmitted by this port to its segment.

Table 67. Port Status information (continued)

Field	Description
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.

Reset Counters for All or Selected Interfaces on the Switch

➢ **To reset the counters for all or selected 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Ports > Port Statistics**.

   The Port Statistics page displays.

6. Select which type of interfaces display onscreen:
   - To display physical ports only, click the **PORTS** link.
   - To display LAGs only, click the **LAGS** link.
   - To display both physical ports and LAGs, click the **All** link.
7. Select one or more interfaces by taking one of the following actions:
   - To clear the statistics for 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 clear the statistics for multiple interfaces, select the check box associated with each interface.
   - To clear the statistics for all interfaces, select the check box in the heading row.
8. Click the **Clear** button.

   The selected counters are reset to 0.

View Detailed Port Statistics

The Port Detailed Statistics page displays a variety of per-port traffic statistics.

➢ **To view detailed port statistics 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Ports > Port Detailed Statistics**.

   The Port Detailed Statistics page displays.

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 view more fields, move the gray bar on the right of the page to the bottom of the page.

The following table describes the detailed port information displayed on the page.

Table 68. Detailed port statistics

Field	Description
ifIndex	This object indicates the ifIndex of the interface table entry associated with this port on an adapter.
Port Type	For normal ports this field displays Normal. Otherwise, the possible values are as follows: • **Mirrored**. The port is participating in port mirroring as a mirrored port. For more information, see *Configure Port Mirroring* on page 308. • **Probe**. The port is participating in port mirroring as the probe port. For more information, see *Configure Port Mirroring* on page 308. • **Port channel**. The port is a member of a link aggregation trunk. For more information, see *Configure Link Aggregation Groups* on page 89.
Port Channel ID	If the port is a member of a port channel, the port channel's interface ID and name are shown. Otherwise, Not a LAG member 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.

Table 68. Detailed port statistics (continued)

Field	Description
STP Mode	The Spanning Tree Protocol administrative mode associated with the port or port channel. The possible values are as follows: • **Enabled**. Spanning Tree Protocol is enabled for this port. • **Disabled**. Spanning Tree Protocol is disabled for this port.
STP State	The port's current Spanning Tree state. This state controls what action a port takes on receipt of a frame. If the bridge detects a malfunctioning port, it places that port into the broken state. The states are defined in IEEE 802.1D: • Disabled • Blocking • Listening • Learning • Forwarding • Broken
Admin Mode	The port control administration state (Up or Down). The port must be enabled for it to be allowed into the network. The default is Up.
LACP Mode	Indicates the Link Aggregation Control Protocol administrative state. The mode must be enabled for the port to participate in link aggregation.
Physical Mode	Indicates the port speed and duplex mode. In autonegotiation mode the duplex mode and speed are set from the autonegotiation process.
Physical Status	Indicates the port speed and duplex mode.
Link Status	Indicates whether the link is up or down.
Link Trap	Indicates whether or not the port sends a trap when link status changes.
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.
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 68. Detailed port statistics (continued)

Field	Description
Packets received > 1024 Octets	The total number of packets received that were in excess of 1024 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.
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) 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) between 64 and 1518 octets, inclusive, but included a bad frame check sequence (FCS) with an integral number of octets.
Overruns	The total number of frames discarded because this port was overloaded with incoming packets, and could not keep up with the inflow.
802.3x Pause Frames Received	A count of MAC control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
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.
Total Packets Transmitted Successfully	The number of frames that were transmitted by this port to its segment.

Table 68. Detailed port statistics (continued)

Field	Description
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.
Total Transmit Errors	The sum of single, multiple, and excessive collisions.
Tx FCS Errors	The total number of packets transmitted with a length (excluding framing bits, but including FCS octets) between 64 and 1518 octets, inclusive, but with a bad FCS with an integral number of octets.
Tx Oversized	The total number of frames that exceeded the maximum permitted frame size. The maximum increment rate of this counter is 815 counts per second at 10 Mb/s.
Total Transmit Packets Discarded	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Excessive Collision Frames	A count of frames for which transmission on a particular interface fails due to excessive collisions.
802.3x Pause Frames Transmitted	A count of MAC control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
EAPOL Frames Received	The number of valid EAPoL frames of any type that were received by this authenticator.
EAPOL Frames Transmitted	The number of EAPoL frames of any type that were transmitted by this authenticator.

View EAP Statistics

Use the EAP Statistics page to display information about Extensible Authentication Protocol (EAP) packets received on a specific port.

➢ **To view EAP statistics and clear the statistics:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Monitoring > Ports > EAP Statistics**.

   The EAP Statistics page displays.
6. To refresh the page with the latest information about the switch, click the **Refresh** button.
7. To clear counters, take one of the following actions:
   - To clear the statistics for a single port, 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 clear all EAP counters for all ports on the switch, 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 69. EAP Statistics information

Field	Description
Port	Selects the port to be displayed. When the selection is changed, a page update occurs causing all fields to be updated for the newly selected port. All physical interfaces are valid.
EAPOL Frames Received	This displays the number of valid EAPoL frames of any type that were received by this authenticator.
EAPOL Frames Transmitted	This displays the number of EAPoL frames of any type that were transmitted by this authenticator.
EAPOL Start Frames Received	This displays the number of EAPoL start frames that were received by this authenticator.
EAPOL Logoff Frames Received	This displays the number of EAPoL logoff frames that were received by this authenticator.
EAPOL Last Frame Version	This displays the protocol version number carried in the most recently received EAPoL frame.
EAPOL Invalid Frames Received	This displays the number of EAPoL frames that were received by this authenticator in which the frame type is not recognized.
EAPOL Length Error Frames Received	This displays the number of EAPoL frames that were received by this authenticator in which the frame type is not recognized.
EAP Response/ID Frames Received	This displays the number of EAP response/identity frames that were received by this authenticator.

Table 69. EAP Statistics information (continued)

Field	Description
EAP Response Frames Received	This displays the number of valid EAP response frames (other than resp/ID frames) that were received by this authenticator.
EAP Request/ID Frames Transmitted	This displays the number of EAP request/identity frames that were transmitted by this authenticator.
EAP Request Frames Transmitted	This displays the number of EAP request frames (other than request/identity frames) that were transmitted by this authenticator.

Perform a Cable Test

Use the Cable Test page to display information about the cables that are connected to switch ports. The cable test is effective for interfaces that can operate at 1G, 2.5G, 5G or 10 Gbps speed.

➢ **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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Ports > Cable Test**.

   The Cable Test page displays.

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, the cable status might be Open Cable or Short Cable because some Ethernet adapters leave unused wire pairs unterminated or grounded.

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

Table 70. Cable Test information

Field	Description
Cable Status	Displays the cable status: • **Normal**. The cable is working correctly. • **Open Cable**. The cable is disconnected or a faulty connector exists. A cable is connected to the port, but it is not connected to the other side (no link). Open Cable status at close to 0 meters (0M) may indicate that no cable is inserted in the port. • **Short Cable**. An electrical short exists in the cable. • **Cable Test Failed**. The cable status could not be determined. The cable might in fact be working. • **Untested**. The cable is not yet tested. • **Invalid cable type**. The cable type is unsupported. • **No cable**. The cable is not present.
Cable Length	The estimated length of the cable in meters. The length is displayed as a range between the shortest estimated length and the longest estimated length. The length is of approximate accuracy (0–50 m, 50–80 m, 80–110 m). Not Supported 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 Cable, Short Cable, or No Cable.

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.

From the **Monitoring > Logs** menu, you can access links to the features described following sections:

- *Manage the Buffered Logs* on page 302
- *Manage the Flash Log* on page 303
- *Manage the Server Log* on page 305
- *View the Trap Logs* on page 307

Manage the Buffered Logs

The buffered log stores messages in RAM memory based on 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 manage and view the buffered logs:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Logs > Buffered Logs**.

   The Buffered Logs Configuration page displays. The page also shows the Buffered Logs section.

6. Select one of the following Admin Status radio buttons:
   - **Enable**. Enable system logging.
   - **Disable**. Prevent the system from logging messages.

   The only selection from the **Behavior** menu is **Wrap**, which means that when the buffer is full, the oldest log messages are deleted as the system logs new messages.

7. Click the **Apply** button.

   Your settings are saved.

   The Total Number of Messages field displays the number of messages the system logged in memory. The 128 most recent entries are displayed on the page.

   The Buffered Logs table displays the log messages. Messages logged to a collector or relayed through the syslog are provided in the following format:

```
10 Oct 2012 14:17:43%AAA-I-DISCONNECT: http connection for user admin, source
10.5.70.19 destination 10.5.234.201 TERMINATED
10 Oct 2012 13:52:00%AAA-I-CONNECT: New http connection for user admin, source
10.5.70.19 destination 10.5.234.201 ACCEPTED
```

The syslog message includes the following fields:

- Date
- Time
- Module (AAA in the previous examples).
- Severity (I in the previous examples).
- Action (DISSCONNECT and CONNECT in the previous examples).
- Description (http connection for user admin, source 10.5.70.19 destination 10.5.234.201 TERMINATED in the first example; http connection for user admin, source 10.5.70.19 destination 10.5.234.201 ACCEPTED in the second example.)

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

➢ **To manage and view the flash log:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Logs > FLASH Logs**.

   The FLASH Log Configuration page displays. The page also shows the FLASH Logs section.

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. The severity can be one of the following levels:

- **Emergency**. The highest warning level. If the device is down, or not functioning properly, an emergency log message is saved to the device.
- **Alert**. 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**. 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**. A device error occurred, such as a port being offline.
- **Warning**. The lowest level of a device warning.
- **Notice**. Normal but significant conditions. Provides the network administrators with device information.
- **Informational**. Provides device information.
- **Debug**. Provides detailed information about the device.

8. Click the **Apply** button.

   Your settings are saved.

   The Total Number of Messages field shows the total number of persistent log messages that are stored on the switch. The 128 most recent entries are displayed on the page.

   The FLASH Logs table displays the log messages, if any.

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

Table 71. FLASH Logs table information

Field	Description
Log Index	An index number for the log message.
Log Time	The time that the message was logged.
Description	The description of the message.

Manage the Server Log

You can allow the switch to send log messages to remote logging hosts configured on the switch.

Add a Remote Syslog Host

A remote syslog host is the same as a remote log server.

➢ **To add a remote syslog host:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Logs > Server Log**.

   The Server Configuration page displays.

6. Specify the following settings:
   - **IP Address Type**. Specify the IP address type of the host, which can be **IPv4**, **IPv6**, or **DNS**.
   - **Host Address**. Specify the IP address or host name of the syslog host.
   - **Port**. Specify the port on the host to which syslog messages must be sent. The default port number is 514.
   - **Severity Filter**. Use the menu to select the severity of the logs that must be sent to the logging host. Logs with the selected severity level and all logs of greater severity are sent to the host. For example, if you select **Error**, the logged messages include Error, Critical, Alert, and Emergency. The default severity level is Alert. The severity can be one of the following levels:
     - **Emergency**. The highest warning level. If the device is down or not functioning properly, an emergency log is saved to the device.
     - **Alert**. The second-highest warning level. An alert log is saved if a serious device malfunction occurs, such as all device features being down.
     - **Critical**. 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**. A device error occurred, such as a port being offline.
- **Warning**. The lowest level of a device warning.
- **Notice**. Provides the network administrators with device information.
- **Informational**. Provides device information.
- **Debug**. Provides detailed information about the log.

7. Click the **Add** button.

   The Status field in the Server Configuration table shows whether the remote logging host is enabled, which it is by default.

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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Logs > Server Log**.

   The Server 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 *Access the Switch* on page 12.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Logs > Server Log**.

   The Server Configuration page displays.

6. Select the check box that is associated with the host.
7. Click the **Delete** button.

   The host is removed.

View the Trap Logs

Use the Trap Logs page to view information about the SNMP traps generated on the switch. The information can be retrieved as a file.

The page also displays information about the traps that were sent.

- **View the trap logs and clear the counters:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Logs > Trap Logs**.

   The Trap Logs page displays.

   The page shows the number of traps that occurred since the switch last rebooted.

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

Configure Port Mirroring

Port mirroring selects the network traffic for analysis by a network analyzer. This is done for specific ports of the switch. As such, many switch ports are configured as source ports and one switch port is configured as a destination port. You can configure how traffic is mirrored on a source port. Packets that are received on the source port, that are transmitted on a port, or are both received and transmitted can be mirrored to the destination port.

The packet that is copied to the destination port is in the same format as the original packet on the wire. This means that if the mirror is copying a received packet, the copied packet is VLAN tagged or untagged as it was received on the source port. If the mirror is copying a transmitted packet, the copied packet is VLAN tagged or untagged as it is being transmitted on the source port.

➢ **To specify one or more source ports and the destination port for port mirroring:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Monitoring > Mirroring > Port Mirroring**.

   The Status Table page displays.

6. Select one or more source ports by taking one of the following actions:
   - To configure a single port as the source port, 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 ports as source ports, select the check box associated with each port.

   Note: You can select only physical ports, not LAGs.

7. From the **Destination Port** menu, select the destination port to which port traffic must be copied.

   You can configure only one destination port, which must be a physical port, not a LAG. The port functions as a probe port and receives traffic from all configured source ports. If no port is configured, none is displayed.

8. From the **Direction** menu, specify the direction of the traffic that must be mirrored from the selected source ports:
   - **Rx only**. The switch monitors received (ingress) packets only.
   - **Tx only**. The switch monitors transmitted (egress) packets only.
   - **Tx and Rx**. The switch monitors transmitted and received packets. This is the default setting.
9. Click the **Apply** button.

   Your settings are saved.

   The Mirroring Port field indicates Mirror for a port that is enabled as the destination port.

View the System Resource Utilization

The switch uses Ternary Content Addressable Memory (TCAM) to support packet actions at wire speed. TCAM holds rules that are produced by various applications. The maximum number of TCAM rules that can be allocated by all applications on the switch is 2048. TCAM is used by the following features:

- ACLs
- DiffServe
- Dynamic VLAN assignment (DVA)
- DHCP snooping

Some applications allocate rules upon their initiation. Additionally, processes that initialize during the system boot allocate some of their rules during the startup process.

The System Resources Utilization page displays the system resource utilization and maximum number of TCAM entries.

➢ **To view the system resource utilization:**

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

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

   If you do not know the IP address of the switch, see *Access the Switch* 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 **Monitor > Mirroring > System Resource Utilization**.

The System Resource Utilization page displays. The page also shows the Used Resources section.

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

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

Table 72. System Resource Utilization and Used Resources information

Field	Description
System Resources Utilization	The percentage of total TCAM utilization on the switch.
Max System Resource Entries	The maximum number of TCAM entries that are available on the switch.
ACLs	The number of TCAM entries that are used by ACLs.
DiffServe	The number of TCAM entries that are used by DiffServe.
DVA	The number of TCAM entries that are used by Dynamic VLAN Assignment (DVA).
DHCP Snooping	The number of TCAM entries that are used by DHCP snooping.

Maintain the Switch and Perform Troubleshooting

8

This chapter covers the following topics:

- *Reboot the Switch*
- *Reset the Switch to Its Factory Default Settings*
- *Export a File From the Switch*
- *Download a File to the Switch*
- *Manage Files*
- *Troubleshooting*

Reboot the Switch

Use the Device Reboot page to reboot the switch.

➢ **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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Reset > Device Reboot**.

   The Device Reboot page displays.

6. Select the check box.
7. Click the **Apply** button.

   The switch reboots.

Reset the Switch to Its Factory Default Settings

Use the Factory Default page to 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 *Access the Switch* 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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Maintenance > Reset > Factory Default**.

   The Factory Default 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

The switch supports system file exports from the switch to a remote system by using either TFTP, HTTP or USB.

The **Maintenance > Export** menu contains links to the features described in the following sections.

- *Export a File to the TFTP Server* on page 313
- *HTTP File Export* on page 315
- *Export a File From the Switch to a USB Device* on page 316

Export a File to the TFTP Server

Use the TFTP File Export page to export configuration (ASCII), log (ASCII), and image (binary) files from the switch to a TFTP server on the network.

➢ **To export a file from the switch to the TFTP server:**

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

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

If you do not know the IP address of the switch, see *Access the Switch* on page 12.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Export > TFTP File Export**.

   The TFTP 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 export 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.
   - **Flash Logs**. The flash logs file.
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 the format specified by the server address type.
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 name for the file to be exported.

    You can enter up to 32 characters. The transfer fails if you do not specify a file name. For an software transfer, use a `.bin` file extension.

11. Select the **Start File Transfer** check box to initiate the file transfer.
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.

HTTP File Export

Use the HTTP File Export page to export files of various types from the switch to the management system through an HTTP session by using your web browser.

➢ **To export a file from the switch to another system by using HTTP:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Export > HTTP File Export**.

   The HTTP File Export page displays.

6. From the **File Type** menu, the only option is **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 export a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name or IP address), and download it to that device.

7. 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.

Export a File From the Switch to a USB Device

Use the USB File Export page to export configuration text files from the switch to a USB device.

➢ **To export a file from the switch to a USB 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Export > USB File Export**.

   The USB File Export. page displays.

6. The File Type list displays the type of file that can be exported, which is a Text Configuration file.

   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 export a working configuration from a device, edit it offline to personalize it for another similar device (for example, change the device name or IP address), and download it to that device.

7. In the **File Path** field, enter the path for the file to export.

   You can enter up to 32 characters. Include the slash or 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 USB directory.

8. In the **USB File** field, enter a name along with path for the file to export.

   You can enter up to 32 characters. The transfer fails if you do not specify a file name.

9. 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

The switch supports system file downloads from a remote system to the switch by using either TFTP, HTTP or USB.

The **Maintenance > Download** menu contains links to the features described in the following sections.

- *Download a File to the Switch Using TFTP* on page 317
- *Download a File to the Switch Using HTTP* on page 319
- *Download a File From a USB Device* on page 320

Download a File to the Switch Using TFTP

You can download an image file or configuration files from a TFTP server to the switch.

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

- The file to download from the TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch contains a path to the TFTP server.

You can also download files by using HTTP. See *Download a File to the Switch Using HTTP* on page 319 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 *Access the Switch* on page 12.

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

   The default password is **password**.

   The System Information page displays.
5. Select **Maintenance > Download > TFTP File Download**.

   The TFTP File Download page displays.
6. From the **File Type** menu, select the type of file:
   - **Software**. The software is the system software image. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots

from the nonactive image. This is a safety feature for faults occurring during the boot upgrade process. The default setting is Software.

With this selection, the switch downloads the new software image and overwrites the nonactive image.

- **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 export 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.

  With this selection, the switch downloads the new configuration and overwrites the existing startup configuration, after which the switch automatically reboots using the new configuration.

7. 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.
8. In the **Server Address** field, enter the IP address of the TFTP server in the format specified by the server address type.
9. In the **Transfer File Path** field, specify the path on the TFTP server where the file is located.

   You can enter up to 32 characters. Include the slash or backslash at the end of the path. A path name with a space is not accepted. Leave this field blank to copy the file from the root TFTP directory.
10. In the **Transfer 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.
11. Select the **Start File Transfer** check box to enable the file transfer.
12. 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.

Download a File to the Switch Using HTTP

Use the HTTP File Download page to download files of various types to the switch through an HTTP session by using your web browser.

➢ **To download a file to the switch using HTTP:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Download > HTTP File Download**.

   The HTTP File Download page displays.

6. From the **File Type** menu, select the type of file:
   - **Software**. The software is the system software image. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the nonactive image. This is a safety feature for faults occurring during the boot upgrade process. The default setting is Software.

     With this selection, the switch downloads the new software image and overwrites the nonactive image.

   - **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 export 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.

     With this selection, the switch downloads the new configuration and overwrites the existing startup configuration, after which the switch automatically reboots using the new configuration.

7. Next to Select File, click the **Browse** button and locate the file that you want to download.
8. 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 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.

Download a File From a USB Device

Use the USB File Download page to download a file to the switch from a USB device.

➢ **To download a file from a USB 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Download > USB File Download**.

   The USB File Download page displays.

6. From the **File Type** menu, select the type of file:
   - **Software**. The software is the system software image. The device boots and runs from the active image. If the active image is corrupted, the system automatically boots from the nonactive image. This is a safety feature for faults occurring during the boot upgrade process. The default setting is Software.

     With this selection, the switch downloads the new software image and overwrites the nonactive image.

   - **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 export 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.

     With this selection, the switch downloads the new configuration and overwrites the existing startup configuration, after which the switch automatically reboots using the new configuration.

7. In the **File Path** field, enter the path for the file to be downloaded.

You can enter up to 32 characters. Include the slash or backslash at the end of the path. A path name with a space is not accepted. Leave this field blank to copy the file from the root USB directory.

8. In the **USB File** field, specify the path and file name for the file that you want to download.

   You can enter up to 32 characters. The transfer fails if you do not specify a file name.

9. Click the **Apply** button.

   The file transfer begins.

   The page displays information about the progress of the file transfer. The page refreshes automatically when the file transfer completes.

Manage Files

The switch maintains two versions of the software (firmware) in permanent storage. One image is the active image, and the second image is the backup image. The active image is loaded during subsequent switch restarts. This feature reduces switch down time when you are upgrading or downgrading the switch software.

The **Maintenance > File Management** menu contains links to the features described in the following sections.

- *Change the Image That Loads During the Boot Process* on page 321
- *View the Dual Image Status* on page 322

Change the Image That Loads During the Boot Process

The Dual Image feature allows the switch to retain two images in permanent storage. Use the Dual Image Configuration page to select which image to load during the next boot cycle and to configure an image description.

A legacy software version can ignore (that is, might not load) a configuration file that is created by a newer software version. When a configuration file created by the newer software version is discovered by the system running an older version of the software, the system displays an appropriate warning.

➢ **To change the image that loads during the boot process and configure an image description:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > File Management > Dual Image Configuration**.

   The Dual Image Configuration page displays.

6. From the **Image Name** menu, select the image that is *not* the image displayed in the Current-active field.

   The Current-active field displays the name of the active image.

7. To specify a name for the selected image, enter one in the **Image Description** field.
8. Select the **Activate Image** check box.
9. Click the **Apply** button.

   Your settings are saved.

Note: After activating an image, you must perform a system reboot of the switch to run the new image. The switch continues running the image shown in the Current-active field until the switch reboots.

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

View the Dual Image Status

The Dual Image Status page shows 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > File Management > Dual Image > Dual Image Status**.

   The Dual Image Status page displays. The page also shows the Dual Image Description section.

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

The following table describes the information available on the page.

Table 73. Dual Image Status information

Field	Description
Image1 Ver	The version of the image1 code file.
Image2 Ver	The version of the image2 code file.
Current-active	The currently active image on this switch.
Next-active	The image to be used on the next restart of this switch.
Image1 Description	The description associated with the image1 code file.
Image2 Description	The description associated with the image2 code file.

Troubleshooting

You can use a ping or a traceroute, and you can perform a memory dump.

The **Maintenance > Troubleshooting** menu contains links to the features described in the following sections.

- *Ping an IPv4 Address* on page 323
- *Ping an IPv6 Address* on page 325
- *Send an IPv4 Traceroute* on page 326
- *Send an IPv6 Traceroute* on page 327
- *Generate Technical Support Information* on page 328
- *Enable Remote Diagnostics* on page 329

Ping an IPv4 Address

You can send a ping request to a specified IPv4 address to check whether the switch can communicate with that address. When you click the **Apply** button, the switch sends a specified number of ping requests and the results are displayed.

Note: A subnet broadcast ping and loopback ping are not supported. The switch cannot ping the special broadcast address 255.255.255.255, the local network broadcast address, or a reachable network broadcast address.

➢ **To configure the ping settings and ping an IPv4 address 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Troubleshooting > Ping IPv4**.

   The Ping IPv4 page displays.

6. In the **IP Address/Host Name** field, enter the IP address or host name of the device that must be pinged.

   The maximum number of characters in a name is 160.

7. In the **Count** field, enter the number of echo requests that must be sent.

   The range is 1 to 15. The default value is 3.

8. In the **Interval** field, enter the time between ping packets in seconds.

   The range is 1 to 60. The default value is 3 seconds.

9. In the **Size** field, enter the size of the ping packet. The range is 0 to 65000. The default value is 0 bytes.
10. Click the **Apply** button.

    The specified address is pinged. The results are displayed below the configurable data in the Results field.

    If a reply to the ping is received, a message similar to the following one is displayed:

    ```
    Reply From IP/Host: icmp_seq = 0. time = xx usec. Tx = x, Rx = x Min/Max/Avg RTT =
    x/x/x msec.
    ```

    If a reply to the ping is not received, a message similar to the following one is displayed:

    ```
    Tx = 1, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec
    ```

Ping an IPv6 Address

This page is used to send a ping request to a specified host name or IPv6 address. You can use this to check whether the switch can communicate with a particular IPv6 station. When you click the **Apply** button, the switch sends a specified number of ping requests and the results are displayed below the configurable data.

➢ **To send an IPv6 ping:**

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

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

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

   If you do not know the IP address of the switch, see *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Troubleshooting > Ping IPv6**.

   The Ping IPv6 page displays.

6. From the **Ping** menu, select the type of ping:
   - **Global**. Pings a global IPv6 address.
   - **Link Local**. Pings a link-local IPv6 address over a specified interface. With this selection, the **Interface** menu displays, and you must select the interface.
7. In the **IPv6 Address/Hostname** field, enter the IPv6 address or host name of the station that must be pinged.

   The format is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. The maximum number of characters is 160.

8. In the **Datagram Size** field, enter the datagram size.

   The valid range is 48 to 2048. The default value is 64 bytes.

9. Click the **Apply** button.

   The specified address is pinged. The results are displayed below the configurable data in the Results field.

   If a reply to the ping is received, a message similar to the following one is displayed:

   ```
   Send count=3, Receive count = n from (IPv6 Address). Average round-trip time = n ms.
   ```

   If a reply to the ping is not received, a message similar to the following one is displayed:

   ```
   Send count = 3, Receive count = 0 from IP/HOST Average round trip time = 680 ms.
   ```

Send an IPv4 Traceroute

Use this page to tell 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. Once you click the **Apply** button, the switch sends a traceroute and the results are displayed below the configurable data.

➢ **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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Troubleshooting > Traceroute IPv4**.

   The Traceroute page displays.

6. In the **IP Address/Hostname** field, enter the IP address or host name of the device for which the path must be discovered.

   The maximum number of characters in a name is 160.

7. In the **Probes Per Hop** field, enter the number of probes per hop.

   The range is 1 to 10. The default value is 3.

8. In the **MaxTTL** field, enter the maximum time to live (TTL) for the destination.

   The range is 1 to 255. The default value is 30.

9. In the **InitTTL** field, enter the initial TTL to be used.

   The range is 1 to 255. The default value is 1.

10. In the **MaxFail** field, enter the maximum number of failures allowed in the session.

    The range is 0 to 255. The default value is 5.

11. In the **Interval (secs)** field, enter the time between probes in seconds.

    The range is 1 to 60. The default value is 3.

12. In the **Port** field, enter the UDP destination port for the probe packets.

    The range is 1 to 65535. The default value is 33434.

13. In the **Size** field, enter the size of the probe packets.

    The range is 64 to 1472. The default value is 64.

14. Click the **Apply** button.

    A traceroute request is sent to the specified IPv4 address or host name. The results are displayed below the configurable data in the Results field.

    If a reply to the traceroute is received, a message similar to the following one is displayed:

```
1 10.5.225.33 20 ms 10 ms 30 ms
2 10.5.225.225 10 ms 10 ms 10 ms
3 192.254.254.3 10 ms 30 ms 20 ms
Hop Count = 3 Test attempt = 9 Test Success = 3
```

Send an IPv6 Traceroute

Use this page to tell the switch to send a traceroute request to a specified IPv6 address or host name. You can use this to discover the paths that packets take to a remote destination. Once you click the **Apply** button, the switch sends a traceroute and the results are displayed below the configurable data.

➢ **To send an IPv6 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Troubleshooting > Traceroute IPv6**.

   The Traceroute IPv6 page displays.

6. In the **IPv6 Address/Host Name** field, enter the IPv6 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 range is 1 to 10. The default value is 3.

8. In the **Max TTL** field, enter the maximum time to live (TTL) for the destination.

   The range is 1 to 255. The default value is 30.

9. In the **InitTTL** field, enter the initial TTL to be used.

   The range is 1 to 255. The default value is 1.

10. In the **MaxFail** field, enter the maximum number of failures allowed in the session.

    The range is 0 to 255. The default value is 5.

11. In the **Interval(secs)** field, enter the time between probes in seconds.

    The range is 1 to 60. The default value is 0.

12. In the **Port** field, enter the UDP destination port for the probe packets.

    The range is 1–65535. The default value is 33434.

13. In the **Size** field, enter the size of the probe packets.

    The range is 64 to 1472. The default value is 64.

14. Click the **Apply** button.

    A traceroute request is sent to the specified IPv6 address or host name. The results are displayed below the configurable data in the Results field.

    If a reply to the traceroute is received, a message similar to the following one is displayed:

```
1 a:b:c:d:e:f:g 9869 usec 9775 usec 10584 usec
2 0:0:0:0:0:0:0:0 0 usec * 0 usec * 0 usec *
Hop Count = p Last TTL = q Test attempt = r Test Success = s.
```

Generate Technical Support Information

The technical support information consists of a list with multiple show commands that provide a broad view of the switch configuration status, as well as the protocol-level status. This information can be used for debug purposes, when multiple configuration and information items are required. You can collect device information with one operation and provide it to technical support engineers.

➢ **To generate technical support 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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Troubleshooting > Tech Support Info**.

   The Tech Support Info page displays.

6. Click the **Generate Request** button.

   Technical support information is exported from the switch and displayed in the text window on the page. You can then select, copy, and paste the information into a text file on your computer.

Enable Remote Diagnostics

Use the Remote Diagnostics page to enable or disable the option to access the switch remotely to perform diagnostics services, for example, through a Telnet connection.

➢ **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 *Access the Switch* on page 12.

   The login window opens.

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

   The default password is **password**.

   The System Information page displays.

5. Select **Maintenance > Troubleshooting > Remote Diagnostics**.

   The Remote Diagnostics page displays.

6. Select the **Enable** radio button.
7. Click the **Apply** button.

   Your settings are saved.

Configuration Examples

A

This appendix covers the following topics:

- *Virtual Local Area Networks (VLANs)*
- *Access Control Lists (ACLs)*
- *Differentiated Services (DiffServ)*
- *802.1X*
- *MSTP*
- *VLAN Routing Interface Configuration Example*

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 100.
- When a tagged packet enters a port, the tag for that packet is unaffected by the default VLAN ID setting. The packet proceeds to the VLAN specified by its VLAN ID tag number.
- If the port through which the packet entered is not a member of the VLAN as specified by the VLAN ID tag, the packet is dropped.
- If the port is a member of the VLAN specified by the packet's VLAN ID, the packet can be sent to other ports with the same VLAN ID.

- Packets leaving the switch are either tagged or untagged, depending on the setting for that port's VLAN membership properties. A U for a given port means that packets leaving the switch from that port are untagged. Inversely, a T for a given port means that packets leaving the switch from that port are tagged with the VLAN ID that is associated with the port.

The example given in this section comprises numerous steps to illustrate a wide range of configurations to help provide an understanding of tagged VLANs.

VLAN Configuration Examples

This example demonstrates several scenarios of VLAN use and describes how the switch handles tagged and untagged traffic.

In this example, you create two new VLANs, change the port membership for default VLAN 1, and assign port members to the two new VLANs:

1. On the Basic VLAN Configuration page (see *Configure VLANs* on page 94), 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 97) 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 100), specify the PVID for ports g1 and g4 so that packets entering these ports are tagged with the port VLAN ID:
   - **Port g1**: PVID 10
   - **Port g4**: PVID 20
4. With the VLAN configuration that you set up, the following situations produce results as described:
   - If an untagged packet enters port 1, the switch tags it with VLAN ID 10. The packet can access port 2 and port 3. The outgoing packet is stripped of its tag to leave port 2 as an untagged packet. For port 3, the outgoing packet leaves as a tagged packet with VLAN ID 10.
   - If a tagged packet with VLAN ID 10 enters port 3, the packet can access port 1 and port 2. If the packet leaves port 1 or port 2, it is stripped of its tag to leave the switch as an untagged packet.
   - If an untagged packet enters port 4, the switch tags it with VLAN ID 20. The packet can access port 5 and port 6. The outgoing packet is stripped of its tag to become an

untagged packet as it leaves port 6. For port 5, the outgoing packet leaves as a tagged packet with VLAN ID 20.

Access Control Lists (ACLs)

ACLs ensure that only authorized users can access specific resources while blocking off any unwarranted attempts to reach network resources.

ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and provide security for the network. ACLs are normally used in firewall routers that are positioned between the internal network and an external network, such as the Internet. They can also be used on a router positioned between two parts of the network to control the traffic entering or exiting a specific part of the internal network. The added packet processing required by the ACL feature does not affect switch performance. That is, ACL processing occurs at wire speed.

Access lists are sequential collections of permit and deny conditions. This collection of conditions, known as the filtering criteria, is applied to each packet that is processed by the switch or the router. The forwarding or dropping of a packet is based on whether or not the packet matches the specified criteria.

Traffic filtering requires the following two basic steps:

1. Create an access list definition.

   The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. Additionally, you can assign traffic that matches the criteria to a particular queue or redirect the traffic to a particular port. A default *deny all* rule is the last rule of every list.

2. Apply the access list to an interface in the inbound direction.

The switch allow ACLs to be bound to physical ports and LAGs. The switch supports MAC ACLs, IPv4 ACLS, and IPv6 ACLs.

Sample MAC ACL 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 264).

   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:
   - **ID**. 1
   - **Action**. Permit
   - **Match Every**. False

- **CoS**. 0
- **Destination MAC**. 01:02:1A:BC:DE:EF
- **Destination MAC Mask**. 00:00:00:00:FF:FF
- **Source MAC**. 02:02:1A:BC:DE:EF
- **Source MAC Mask**. 00:00:00:00:FF:FF
- **VLAN ID**. 2

For more information about MAC ACL rules, see *Configure MAC ACL Rules* on page 266.

3. On the MAC Binding Configuration page, assign the Sales_ACL to ports 6, 7, and 8, and then click the **Apply** button. (See *Configure MAC Bindings* on page 270.)

   You can assign an optional sequence number to indicate the order of this access list relative to other access lists if any are already assigned to this interface and direction.

4. The MAC Binding Table displays the interface and MAC ACL binding information. (See *View or Delete MAC ACL Bindings in the MAC Binding Table* on page 271.)

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.

Sample Standard IP ACL Configuration

The following example shows how to create an IP-based ACL that prevents any IP traffic from the Finance department from being allowed on the ports that are associated with other departments. Traffic from the Finance department is identified by each packet's network IP address.

1. On the IP ACL page, create a new IP ACL with an IP ACL ID of 1. (See *Configure an IP ACL* on page 272.)
2. On the IP Rules page, create a rule for IP ACL 1 with the following settings:
   - **Rule ID**. 1
   - **Action**. Deny
   - **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 274.
3. Click the **Add** button.
4. On the IP Rules page, create a second rule for IP ACL 1 with the following settings:

- **Rule ID**. 2
- **Action**. Permit
- **Match Every**. True

5. Click the **Add** button.
6. On the IP Binding Configuration page, assign ACL ID 1 to ports 2, 3, and 4, and assign a sequence number of 1. (See *Configure IP ACL Interface Bindings* on page 286.)

   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 288)

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 attempts to deliver the data in a timely fashion. 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)
- IP Service Type octet (also known as ToS bits, Precedence value, DSCP value)
- Layer 4 protocol (TCP, UDP and so on)
- Layer 4 source/destination ports
- Source/destination IP address

From a DiffServ point of view, two types of classes exist:

- DiffServ traffic classes
- DiffServ service levels/forwarding classes

DiffServ Traffic Classes

With DiffServ, you define which traffic classes to track on an ingress interface. You can define simple BA classifiers (DSCP) and a wide variety of multifield (MF) classifiers:

- Layer 2; Layers 3, 4 (IP only)
- Protocol-based
- Address-based

You can combine these classifiers with logical AND or OR operations to build complex MF-classifiers (by specifying a class type of *all* or *any*, respectively). That is, within a single class, multiple match criteria are grouped together as an AND expression or a sequential OR expression, depending on the defined class type. Only classes of the same type can be nested; class nesting does not allow for the negation (*exclude* option) of the referenced class.

To configure DiffServ, you must define service levels, namely the forwarding classes/PHBs identified by a given DSCP value, on the egress interface. You define these service levels by configuring BA classes for each.

Creating Policies

Use DiffServ policies to associate a collection of classes that you configure with one or more QoS policy statements. The result of this association is referred to as a policy.

From a DiffServ perspective, two types of policies exist:

- **Traffic Conditioning Policy**. A policy applied to a DiffServ traffic class
- **Service Provisioning Policy**. A policy applied to a DiffServ service level

You must manually configure the various statements and rules used in the traffic conditioning and service provisioning policies to achieve the desired Traffic Conditioning Specification (TCS) and the Service Level Specification (SLS) operation, respectively.

Traffic Conditioning Policy

Traffic conditioning pertains to actions performed on incoming traffic. Several distinct QoS actions are associated with traffic conditioning:

- **Dropping**. Drops 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**. Marks or remarks the DiffServ code point in a packet with the DSCP value representing the service level associated with a particular DiffServ traffic class.
- **Marking CoS (802.1p)**. Sets the 3-bit priority field in the first/only 802.1p header to a specified value when packets are transmitted for the traffic class. An 802.1p header is inserted if it does not already exist. This is useful for assigning a Layer 2 priority level based on a DiffServ forwarding class (such as the DSCP or IP precedence value) definition to convey some QoS characteristics to downstream switches that do not routinely look at the DSCP value in the IP header.
- **Policing**. A method of constraining incoming traffic associated with a particular class so that it conforms to the terms of the TCS. Special treatment can be applied to out-of-profile packets that are either in excess of the conformance specification or are nonconformant. The DiffServ feature supports the following types of traffic policing treatments (actions):
  - **Drop**. The packet is dropped.
  - **Mark CoS**. The 802.1p user priority bits are marked or remarked and forwarded.
  - **Mark DSCP**. The packet DSCP is marked or remarked and forwarded.
  - **Send**. The packet is forwarded without DiffServ modification.
- **Color mode awareness**. Policing in the DiffServ feature uses either color blind or color aware mode. Color blind mode ignores the coloration (marking) of the incoming packet. Color aware mode takes into consideration the current packet marking when the switch determines the policing outcome. An auxiliary traffic class is used in conjunction with the policing definition to specify a value for one of the 802.1p, IP DSCP, or IP precedence fields designating the incoming color value to be used as the conforming color. You can also specify the color of traffic that exceeds the threshold.
- **Counting**. Updating octet and packet statistics to keep track of data handling along traffic paths within DiffServ. In this DiffServ feature, counters are not explicitly configured by the

user, but are designed into the system based on the DiffServ policy being created. For more information, see *Monitor the Switch and the Ports* on page 291.

- **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.

DiffServ Example Configuration

To create a DiffServ class and policy and attach them to a switch interface, follow these steps:

1. On the QoS Class Configuration page, create a new class with the following settings:
   - **Class Name**. Class1
   - **Class Type**. All

   For more information about this page, see *Configure IPv4 DiffServ Classes* on page 199.
2. Click the **Class1** hyperlink to view the DiffServ Class Configuration page for this class.
3. Configure the following settings for Class1:
   - **Protocol Type**. UDP
   - **Source IP Address**. 192.12.1.0.
   - **Source Mask**. 255.255.255.0.
   - **Source L4 Port**. Other, and enter 4567 as the source port value.
   - **Destination IP Address**. 192.12.2.0.
   - **Destination Mask**. 255.255.255.0.
   - **Destination L4 Port**. Other, and enter 4568 as the destination port value.

   For more information about this page, see *Configure IPv4 DiffServ Classes* on page 199.
4. Click the **Apply** button.
5. On the Policy Configuration page, create a new policy with the following settings:
   - **Policy Selector**. Policy1
   - **Member Class**. Class1

   For more information about this page, see *Configure a DiffServ Policy* on page 207.
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

- **Committed Burst Size**. 128 KB
- **Confirm Action**. Send
- **Violate Action**. Drop

For more information about this page, see *Configure a DiffServ Policy* on page 207.

9. On the Service Configuration page, select the check box next to interfaces 7 and 8 to attach the policy to these interfaces, and then click the **Apply** button. (See *Configure DiffServ Service Interfaces* on page 212.)

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 and burst size of 128 KB. Packets that violate the committed rate and burst size are dropped.

802.1X

Local area networks (LANs) are often deployed in environments that permit unauthorized devices to be physically attached to the LAN infrastructure, or permit unauthorized users to attempt to access the LAN through equipment already attached. In such environments 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, a third role exists:

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.

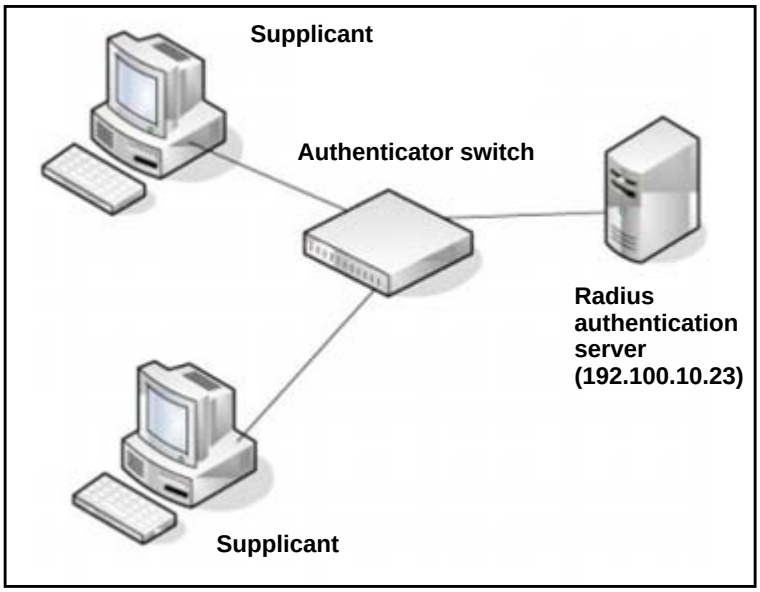


Figure 1. 802.1X authentication roles

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 (mg7–mg8). 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 **mg6** through **mg8**.
2. From the **Port Control** menu, select **Auto**.

   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 mg7–mg8, 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 249 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 click the **Apply** button. (See *Configure Global 802.1X Settings* on page 241.)

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 *Configure RADIUS Servers* on page 218.
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 227.)

This example enables 802.1X-based port security on the switch and prompts the hosts connected on ports mg7–mg8 for an 802.1X-based authentication. The switch passes the authentication information to the configured RADIUS server.

MSTP

Spanning Tree Protocol (STP) runs on bridged networks to help eliminate loops. If a bridge loop occurs, the network can become flooded with traffic. IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) supports multiple instances of spanning tree to efficiently channel VLAN traffic over different interfaces. Each instance of the spanning tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree, with slight modifications in the working but not the end effect (chief among the effects is the rapid transitioning of the port to the forwarding state).

The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full-duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to the Forwarding state and the suppression of Topology Change Notification. These features are represented by the parameters pointtopoint and edgeport. MSTP is compatible to both RSTP and STP. It behaves in a way that is appropriate for STP and RSTP bridges.

An MSTP bridge can be configured to behave entirely as a RSTP bridge or an STP bridge. So, an IEEE 802.1s bridge inherently also supports IEEE 802.1w and IEEE 802.1D.

The MSTP algorithm and protocol provide simple and full connectivity for frames assigned to any given VLAN throughout a bridged LAN comprising arbitrarily interconnected networking devices, each operating MSTP, STP, or RSTP. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) regions composed of LANs and or MSTP bridges. These regions and the other bridges and LANs are connected into a single Common Spanning Tree (CST). (IEEE DRAFT P802.1s/D13)

MSTP connects all bridges and LANs with a single Common and Internal Spanning Tree (CIST). The CIST supports the automatic determination of each MST region, choosing its maximum possible extent. The connectivity calculated for the CIST provides the CST for interconnecting these regions, and an Internal Spanning Tree (IST) within each region. MSTP ensures that frames with a given VLAN ID are assigned to one and only one of the MSTIs or the IST within the region, that the assignment is consistent among all the networking devices in the region, and that the stable connectivity of each MSTI and IST at the boundary of the region matches that of the CST. The stable active topology of the bridged LAN with respect to frames consistently classified as belonging to any given VLAN thus simply and fully connects all LANs and networking devices throughout the network, though frames belonging to different VLANs can take different paths within any region, per IEEE DRAFT P802.1s/D13.

All bridges, whether they use STP, RSTP, or MSTP, send information in configuration messages through Bridge Protocol Data Units (BPDUs) to assign port roles that determine each port's participation in a fully and simply connected active topology based on one or more spanning trees. The information communicated is known as the spanning tree priority vector. The BPDU structure for each of these different protocols is different. An MSTP bridge transmits the appropriate BPDU depending on the received type of BPDU from a particular port.

An MST region comprises of one or more MSTP bridges with the same MST configuration identifier, using the same MSTIs, and without any bridges attached that cannot receive and transmit MSTP BPDUs. The MST configuration identifier includes the following components:

1. Configuration identifier format selector
2. Configuration name
3. Configuration revision level
4. Configuration digest: 16-byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID to MSTID mapping)

Because multiple instances of spanning tree exist, an MSTP state is maintained on a per-port, per-instance basis (or on a per-port, per-VLAN basis, as any VLAN can be in one and only one MSTI or CIST). For example, port A can be forwarding for instance 1 while discarding for instance 2. The port states changed since IEEE 802.1D specification.

To support multiple spanning trees, configure an MSTP bridge with an unambiguous assignment of VLAN IDs (VIDs) to spanning trees. For such a configuration, ensure the following:

1. The allocation of VIDs to filtering identifiers (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 g1–mg5 are connected to host stations, so those links are not subject to network loops. Ports mg6–mg7 are connected across switches 1, 2, and 3.

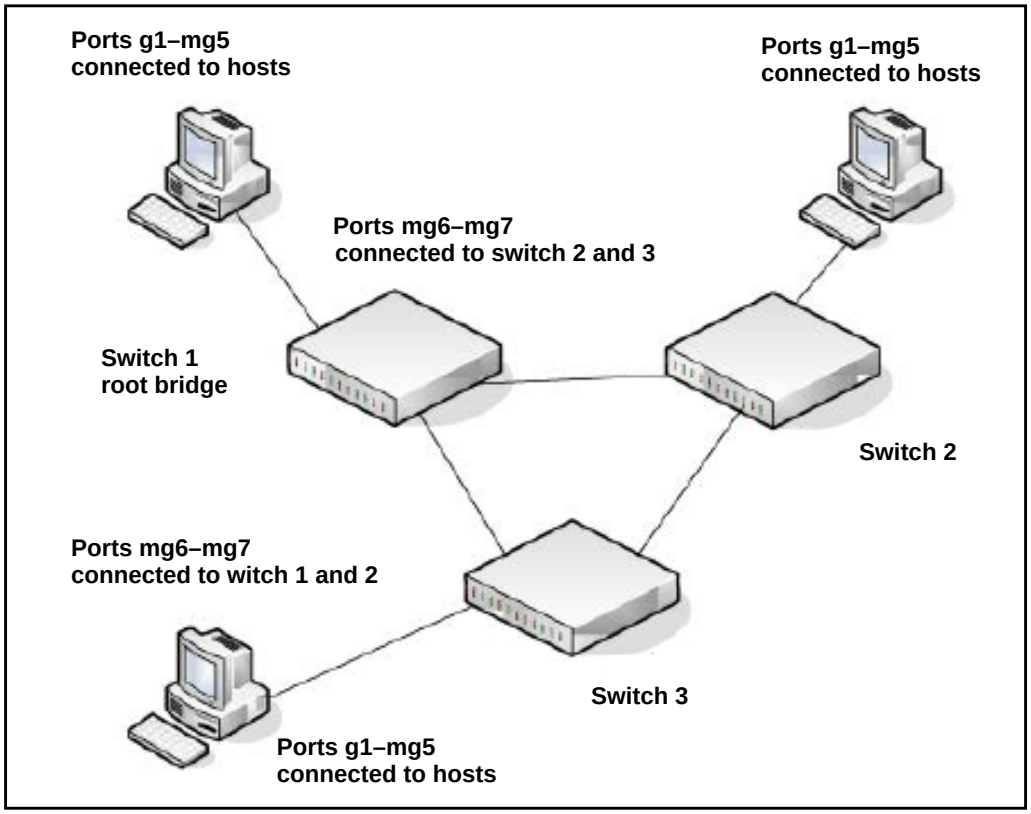


Figure 2. MSTP sample configuration

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 95).
2. On the VLAN Membership page, include ports g1–mg7 as tagged (T) or untagged (U) members of VLAN 300 and VLAN 500 (see *Configure VLAN Membership* on page 97).
3. On the STP Configuration page, enable the Spanning Tree State option (see *Configure STP Settings* on page 116).

   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 CST Settings* on page 118).
5. On the CST Port Configuration page, select ports g1–mg7 and select **Enable** from the **STP Status** menu (see *Configure CST Port Settings* on page 120).
6. Click the **Apply** button.
7. Select ports g1–mg5 (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 *Manage MST Settings* on page 124.
10. Click the **Add** button.
11. Create a second MST instance with the following settings
    - **MST ID**. 2
    - **Priority**. 49152
    - **VLAN ID**. 500
12. Click the **Add** button.

In this example, assume that switch 1 became the root bridge for the MST instance 1, and switch 2 became the root bridge for MST instance 2. Switch 3 supports hosts in the sales department (ports g1, g2, and g3) and in the HR department (ports g4 and mg5). 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.

VLAN Routing Interface Configuration Example

VLANs divide broadcast domains in a LAN environment. When hosts in one VLAN must communicate with hosts in another VLAN, the traffic must be routed between them. This is known as inter-VLAN routing. On the switch, it is accomplished by creating Layer 3 interfaces (switch virtual interfaces [SVI]).

When a port is enabled for bridging (the default) rather than routing, all normal bridge processing is performed for an inbound packet, which is then associated with a VLAN. Its MAC destination address (MAC DA) and VLAN ID are used to search the MAC address table. If routing is enabled for the VLAN, and the MAC DA of an inbound unicast packet is that of the internal bridge-router interface, the packet is routed. An inbound multicast packet is forwarded to all ports in the VLAN, plus the internal bridge-router interface, if it was received on a routed VLAN.

Because a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. VLAN routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when additional segmentation or security is required.

Complete these steps to configure a switch to perform interVLAN routing:

1. Use the IP Configuration page to enable routing on the switch.

   For more information about this step, see *Configure the IPv4 Address for the Network Interface and Management VLAN* on page 28.

2. Determine the IP addresses that you want to assign to the VLAN interface on the switch.

   For the switch to be able to route between the VLANs, the VLAN interfaces must be configured with an IP address. When the switch receives a packet destined for another subnet/VLAN, the switch looks at the routing table to determine where to forward the packet. The packet is then passed to the VLAN interface of the destination. It is then sent to the port where the end device is attached.

3. Use the VLAN Routing Wizard page to create a routing VLAN, configure the IP address and subnet mask, and add the member ports.

   For more information about this step, see *Use the VLAN Static Routing Wizard* on page 162.

4. Use the VLAN Routing Configuration page to view or modify the VLAN as a routing VLAN.

   In the following figure, VLAN 30 is a routing VLAN with IP address 10.1.1.1 and subnet mask 255.255.255.0. (For more information about this page, see *VLAN Routing Configuration* on page 163.)

Hardware Specifications and Default Settings

B

This appendix covers the following topics:

- *Hardware Specifications*
- *Switch Default Settings*

Hardware Specifications

Table 74. Hardware specifications

Feature	Description
Interfaces	Nine Ethernet RJ-45 ports and one fiber SFP+ ports: • **Ports g1–g4**. 1 Gbps Ethernet ports • **Ports mg5–mg6**. 2.5 Gbps Multi-Gigabit Ethernet ports • **Ports mg7–mg8**. 5 Gbps Multi-Gigabit Ethernet ports • **Port xmg9**. 10 Gbps Multi-Gigabit Ethernet port • **Port xg10**. Fiber port (SFP+)
Flash memory size	256 MB NAND
SDRAM size and type	512 MB DDR3 SDRAM
Switching capacity	Non blocking full wire speed on all packet sizes
Forwarding method	Store and forward
Packet forwarding rate	• **1G**. 1,488,000 pps • **2.5G**. 3,720,000 pps • **5G**. 7,440,000 pps • **10G**. 14,880,000 pps
MAC addresses	16 K
Green Ethernet	• Automatic power-down mode on a port when the link is down • Short cable mode • EEE mode
Supported protocols and standards	• TCP/IP • UDP • HTTP • ICMP • TFTP • DHCP • IEEE 802.1D • IEEE 802.1 p • IEEE 802.1Q • IEEE802.3 1000BASE-T and 10GBASE-T • IEEE802.3az (EEE) • IEEE 802.3bz NBASE-T and MGBASE-T • IEEE 802.1af (PoE) • IEEE 802.1at (PoE+) • IEEE 802.3ad Link aggregation (LAG with LACP) • IEEE 802.1ab LLDP • IEEE 802.1x RADIUS network access control

Switch Default Settings

Table 75. Switch default settings

Feature	Sets Supported	Default Setting
Auto negotiation/static speed/duplex	All ports	Auto-negotiation
Auto MDI/MDIX	N/A	Enabled
802.3x flow control/back pressure	1 (per system)	Disabled
Port mirroring	1 destination port and 8 source ports	Disabled
Link aggregation groups (LAGs)	8	Preconfigured
802.1D spanning tree	1	Disabled
802.1w RSTP	1	Enabled
802.1s spanning tree	16 instances	Disabled
Static 802.1Q tagging	256	Default VLAN ID = 1
Learning process	Supports static and dynamic MAC entries	Dynamic learning is enabled by default
Storm control per each packet type (unicast, broadcast, multicast)	All ports	Disabled
Jumbo frame	All ports	Enabled. Maximum frame size is 10 KB
Number of queues	8	N/A
Port based	N/A	N/A
802.1p	8	Enabled
DSCP	64	Disabled
Rate limiting	All ports	Disabled
802.1x	All ports	Disabled
MAC ACL	164 (shared with IP and IPv6 ACLs)	All MAC addresses allowed
IP ACL	164 (shared with MAC and IPv6 ACLs)	All IP addresses allowed
IPv6 ACL	164 (shared with IP ACL and MAC ACL)	All IP addresses allowed
Password control access	1	Idle time-out is 10 minutes The password is **password**
Management security	1 profile with 20 rules for HTTP/HTTPS/SNMP access to allow or deny an IP address or subnet	All IP addresses allowed

Table 75. Switch default settings (continued)

Feature	Sets Supported	Default Setting
Port MAC lock down	All ports	Disabled
Boot code update	Boot code is automatically updated together with firmware upgrade.	N/A
DHCP/static IP	1	DHCP enabled/192.168.0.239
Default gateway	1	192.168.0.254
System name configuration	1	NULL
Configuration save/restore	1	N/A
Firmware upgrade	1	N/A
Factory default reset	1 (web and front-panel button)	N/A
Dual image support	1	Enabled
Multisession web connections	5	Enabled
SNMPv1/V2c SNMP v3	Maximum 5 community entries	Disabled
Time control	1 (Local or SNTP)	Local time enabled
LLDP/LLDP-MED	All ports	Enabled
Logging	4 (buffered, flash, server & traps)	Buffer log enabled
MIB Support	1	Enabled
Smart Control Center	N/A	Enabled
Statistics	N/A	N/A
IGMP snooping v1/v2/v3	All VLANs	Disabled
IGMP Snooping Querier	All VLANs	Disabled
Configurations upload/download	1	N/A
EAPoL flooding	All ports	Disabled
STP BPDU flooding	All ports	Disabled
LLDP PDU flooding	All ports	Disabled
Multicast groups	512	Disabled
Filter multicast control	1	Disabled
Number of static routes	32 for IPv4 and IPv6, each	N/A
Number of routed VLANs	16 for IPv4 and IPv6, each	N/A
Number of ARP cache entries	512	N/A

Table 75. Switch default settings (continued)

Feature	Sets Supported	Default Setting
Number of DHCP snooping bindings	1024	N/A
Number of DHCP static entries	1024	N/A
MLD snooping v1/v2	All VLANs	Disabled
MLD Snooping Querier	All VLANs	Disabled
Private VLAN	Primary, Community and Isolated	Disabled
GVRP	All ports	Disabled
Protocol-based VLANs	8	Disabled
MAC-based VLANS	8	Disabled
OUI-based Voice VLANS	All ports	Disabled
Auto-VoIP	All ports	Disabled
IP MTU settings	Up to 9000. Globally per IPv4 and IPv6	1500
USB port and USB flash device	1	N/A
PoE+ ports (model MS510TXPP only)	8	N/A